Error 404: Government not Secure

A cross-country empirical analysis of the relationship between cybersecurity and e-government development

Joeri M. Nelemans | 374506

12-7-2019

MSc International Public Management and Policy

Thesis supervisor/first reader: Dr B. George

Erasmus School of Social and Behavioural Sciences

Second reader: Dr. M. Onderco

Erasmus University Rotterdam

Word count: 23.361

Abstract

Technological developments in the last few decades have created countless opportunities for society, shifting not only economic, but also governmental activities to the digital realm, resulting in the development of e-government. However, these new opportunities present new risks, as recent large-scale cyber-attacks on governmental institutions have shown. The objective of this study is to explore the relationship between cybersecurity on the one hand, and the development of e-government on the other, to provide better insight in the relationship between these increasingly important phenomena within society. Based on the literature, five individual components of cybersecurity have been identified, which were all expected to have a positive relationship with the development of e-government, namely 'legal', 'technical', 'organisational', 'capacity-building' and 'cooperation'. To test the existence and strength of these relationships, a panel dataset was created out of six existing databases: the Global Cybersecurity Index (GCI), the UN E-Government Development Index (EGDI), the Corruption Perception Index (CPI), the Global Innovation Index (GII), the Democracy Index and the World Bank database. This panel dataset consisted of data on e-government development, the five cybersecurity components and 3 control variables, of 193 countries in the years of 2014 and 2016. With this panel dataset, a pooled OLS regression analysis was conducted. The results of this analysis indicate that the 'legal' and 'technical' component of cybersecurity have a significant positive association with the development of e-government. This study has not found a significant relationship between the 'organisational', 'capacity-building' and 'cooperation' components of cybersecurity and e-government development. Additionally, the study found a significant positive relationship between 'national income' as control variable, and e-government development. This study therefore concludes that there is a differentiated relationship between the various individual components of cybersecurity and the development of e-government. These results have scientific implications because they contribute to the discussion in the literature about the theoretical underpinning of the relationship between the concepts of cybersecurity and e-government development, and the more underlying relationship between security and development. These results also have societal implications, as they provide policymakers and governments insight into the cybersecurity determinants for the successful development of e-government services.

Acknowledgements

Hereby, I proudly present my master thesis for International Public Management & Policy: *Error 404: Government not Secure*. Having finished this thesis means having finished two master programmes (the other one being Crisis & Security Management), which I have chosen based on my interest in both security and international relations/cooperation, and the combination hereof. By looking at cybersecurity in the context of an international comparison, I believe this thesis represents this interest well. This made conducting this research a truly interesting and enjoyable exercise, not only an essential educational one. It has piqued my interest and increased my knowledge concerning this, and related topics, which I am sure will help me in my further career.

At the start, this thesis seemed to be one of the biggest challenges in my academic career, mainly because of limited time and a research methodology out of my comfort zone. Nevertheless, with incredible assistance and support, as well as a lot of hard work, I can happily say that I did it. I want to express my gratitude especially to my supervisor, Dr. Bert George, for feedback, tips and continuous assistance throughout the process. I want to highlight in particular the way you convinced me that statistics is *not* scary and incomprehensible, which made me believe that (with the right assistance) even I could do it. Furthermore, I would like to thank Dr. Michal Onderco for his helpful feedback and assistance as second reader. Additionally, I would like to thank my friends Tamim and Michelle, the former for his valuable input regarding the idea for this research and the latter for regularly assisting me with a critical eye and helpful tips. Lastly, I want to thank my girlfriend Saskia, for her tips and mental support but mostly her belief in me from start to end.

Joeri Nelemans

Rotterdam, July 2019

Contents

List of tables & figures

List of abbreviations

ASPA	American Society for Public Administration
CIRT	Computer Incident Response Team
CPI	Corruption Perception Index
CSB	Common Source Bias
DPADM	Division for Public Administration and Development Management
DPKO	Department of Peacekeeping Operations
DV	Dependent Variable
EGDI	E-Government Development Index
ESS	European Security Strategy
EU	European Union
GCI	Global Cybersecurity Index
GII	Global Innovation Index
HCI	Human Capital Index
ICT	Information and Communication Technology
IR	International Relations
ITU	International Telecommunications Union
IV	Independent Variable
NPG	New Public Governance
NPM	New Public Management
OECD	Organisation for Economic Co-operation and Development
OLS	Ordinary Least Squares
OSI	Online Service Index
SDG	Sustainable Development Goal
SIDS	Small Island Developing States
SSA	Sub-Saharan Africa
TII	Telecommunication Infrastructure Index
UN	United Nations
UNDESA	United Nations Department of Economic and Social Affairs
UNDP	United Nations Development Programme
UNV	United Nations Volunteer
USD	United States Dollar
WIPO	World Intellectual Property Organization

1 Introduction

1.1 Problem statement

The movable type-printing press in the fifteenth century, the telegraph in 1844, the telephone in 1876, the radio in the 1920s, television broadcasting in 1946, and the rise of the Internet in the 1980s. Next to changing the landscape of information access, all these technological revolutions have also changed government service delivery (West, 2004). This last revolution, the emergence of the Internet, has made it possible for public administrations around the world, to adopt web-based technologies in order to deliver government services (Bekkers, 2003; Torres, Pina, & Royo, 2005). This introduction, management and use of information and communication technologies (ICTs) by the public sector is widely known as 'e-government' (Lips & Schuppan, 2009). E-government is defined by the World Bank (2001) as *"government-owned or operated systems of information and communications technologies (ICTs) that transform relations with citizens, the private sector and/or other government agencies so as to promote citizen empowerment, improve service delivery, strengthen accountability, increase transparency, or improve government efficiency"*. This definition portrays some characteristics of e-government, that are connected with another major revolution, not in technology, but in public administration: New Public Management (NPM). E-government inherits the administrative reform policies inspired by NPM reforms since the 1980s (Torres, Pina & Royo, 2005).

Until the late 70s of the 20th century, public administration largely took place according to the traditional model of bureaucracy, extensively elaborated on by for instance Max Weber and Woodrow Wilson. The idea of an impartial, professional and bureaucratic organisation that executes the policy separately from politics, was the central idea on how public administration should take shape (Hughes, 2003). From the late 1970s onwards, this idea changed fundamentally. New Public Management (NPM) has been the most striking international development in the field of public administration (Hood, 1991). Pushed by post-World War II societal forces and economic/managerial reforms, NPM introduced a new way of public management, aimed at downsizing and increasing the efficiency of governments (Hood, 1991). Since the NPM reforms, governments within the world of the Organisation for Economic Co-operation and Development (OECD) have taken on a more 'private sector way of working', by focussing on functional ideas of expediency, efficiency, economy and calculation of ends

(Homburg & Bekkers, 2004). In the 1980s and 1990s, shortly after the emergence of NPM, technological development enabled the Internet to become a large scale medium for the general public (Koops, 2011). Empowered by this uptake of the Internet in society, the private sector expanded their activities by entering into the realm of 'e-commerce' or 'e-business' (Lips & Schuppan, 2009). Governments were not far behind and also expanded their service delivery to the world of internet technology, which resulted in e-government. However, looking at all the countries in the world, there is a high variety concerning the development of e-government. The e-government of developing countries for instance, lags behind on most of the developed world (Verkijika and De Wet, 2016).

Next to the development of e-government, the emergence of the Internet also created a new security concern for governments, namely 'cybersecurity'. Because of the process of digitalisation, a significant amount of human activities have shifted to the digital infrastructures of the Internet, also known as the 'cyberspace' (Onumo, Cullen, & Ullah-Awan, 2017). We as human beings rely increasingly on the digital infrastructure for the storage of data and the delivery of key services (Pupillo, 2018). The data within this digital infrastructure is vulnerable and susceptible to cyber threats, such as cybercrime and cyberattacks (Pupillo, 2018). In the past few years, there has been an increase in the number of cyber-attacks, of which WannaCry and Petya are two well-known examples. Especially WannaCry was worrisome for many governments as it hit 150 countries among which government services like the British National Health Service (BBC, 2017). Examples like these, but also smaller scale threats and risks, such as cyber criminals and human errors[1] are a serious concern for governments, who are faced with an increasing amount and complexity of cyber challenges (Sutherland, 2018). An increasing amount of critical public sectors, such as the financial sector and the energy sector, provide and operate their services through web-based systems, which consequently makes cybersecurity an increasingly important policy concern for governments. Examples such as Russia's attacks on the networks of the US Democratic Party in 2016 and more recent attempts to influence European elections, but also the cyber-attack on a Ukrainian power grid in 2015, show the public security risks cyber threats pose. These cyber-threats to critical infrastructure and democracy make cybersecurity a growing security policy issue (Carr, 2016). So while on the one hand the

[1] Human errors in the context of cybersecurity are instances in which a cyber threat emerges because of human behaviour. This can for instance be negligence in the handling of unencrypted USB sticks and other data carriers (Sutherland, 2018: p. 1).

development of online government services continues, cybersecurity becomes a growing concern and is the talk of the town (Pupillo, 2018).

Evidence from studies all over the world demonstrate that e-government is a highly valuable governmental strategy to increase the efficiency of public services, gain citizens' trust, counter public sector corruption and move towards more democratic governance (Verkijika & De Wet, 2016). The successful development of these e-government services is subject to many factors, among which the development of a sufficient level of cybersecurity. Next to the existence and usage of online governmental services, e-government development entails the development and readiness of a country's telecommunications infrastructure and human capacity (United Nations, 2018). Cybersecurity on the other hand, knows five building blocks, (or pillars): legal, technical, organisational, capacity-building and cooperation (ITU, 2018). Although a collaborative development of both cybersecurity and e-government is necessary, the development of the former has not kept up with the development of the latter, according to Onumo, Cullen and Ullah-Awan (2017). Cyber-offenders (whether criminal, political or state-driven) are often well ahead of state digital law enforcement legislation, institutions and cyber policies (Botchwey, 2018). This does not only have consequences for a country's e-economy, but also for e-government. An important reason why cybersecurity is connected to e-government – at least from a user's (citizen's) perspective – is that a high level of cybersecurity reassures confidence in the use of e-government services (Onumo, Cullen, & Ullah-Awan, 2017; Verkijika & De Wet, 2016). Thus, a high level of cybersecurity is important for a well-functioning e-government, because it fosters a large degree of digital participation by citizens (e-citizens). So while Pupillo (2018) claims that technological progress and digitalisation (e.g. e-government) makes our society more vulnerable and fragile, cybersecurity could be the panacea that is able to break this 'paradox of progress'. This study will therefore investigate the relationship between cybersecurity and e-government development.

1.2 Objective of the study

The objective of this research is to contribute to a better understanding of how different levels of cybersecurity relate to differentiation in the development of e-government within countries all over the world. In previous studies, cybersecurity is presented as a potential explanatory factor for this differentiation (Onumo, Cullen & Ullah-Awan, 2017; Verkijika & De Wet, 2016). As such, this study will also look at the relationship between cybersecurity and e-government development, but with a specific focus on the components of cybersecurity, and their separate relationship with the development of e-government. By breaking down the concept of cybersecurity into sub-concepts, this study will help provide a more in-depth understanding of the relationship between cybersecurity and e-government development.

This study will conduct a statistical analysis, in the shape of a Pooled Ordinary Least Squared (OLS) regression analysis, to answer the research question and investigate whether the relationship between cybersecurity and e-government is significant. For the regression analysis, this study will use a set of panel data, which is extracted from six existing databases. For the data on cybersecurity, the Global Cybersecurity Index (GCI) by the International Telecommunications Union (ITU) will be used. Surveys for the GCI by the ITU have been conducted in three years, 2014, 2017 and 2018. Because of the unavailability of the data from 2018 (see chapter 4), only the data from 2014 and 2016 will be used. The GCI measures national cybersecurity by examining its member states' commitment on a set of 25 indicators, distributed over five pillars. For the data on the development of e-government, this study will make use of the United Nations E-government Development Index (EGDI). This is a (mostly) biannual index, of which the first publication stems from 2001, which measures national e-government readiness and development on the basis of three sub-indexes: the Online Service provision Index (OSI), the Telecommunication Infrastructure Index (TII) and the Human Capital Index (HCI). This study will make us of the data of the 2014 and 2016 EGDI editions. The different editions of both the GCI and the EGDI were scanned to check for methodological consistency (see chapter 4). For the control variables, which are selected on the basis of a literature review, this study will make use of data retrieved from the World Bank, the Corruption Perception Index (CPI) by Transparency International, the Democracy Index by The Economist Intelligence Unit and the Global Innovation Index (GII) by a joint venture between the World Intellectual Property Organization (WIPO), Cornell University and INSEAD.

1.3 Research questions

To be able to investigate the relationship between cybersecurity and e-government, and obtain the research objective, this study will address the following research question:

To what extent can the difference in e-government development around the world be explained by cybersecurity?

Answering the main research question will be done by answering the following sub-questions:

1. What does the literature say about the concepts ‘e-government development’ and ‘cybersecurity’?
2. What is, according to the literature, the theoretical relationship between cybersecurity and e-government development?
3. What is the state of cybersecurity in a global context?
4. What is the state of e-government development in a global context?
5. Can the theoretical relationship between cybersecurity and e-government development be confirmed in a global context?

1.4 Relevance

1.4.1 Societal relevance

“Over the last two decades, the Internet and more broadly, cyberspace, has had a tremendous impact on all parts of society. […] An open and free cyberspace has promoted political and social inclusion worldwide […].” (European Commission, 2013: p. 2). This is part of the introduction of the Cybersecurity Strategy of the European Union, drafted in 2013. It pinpoints exactly how the recent digitalisation has led to an immense involvement of the Internet (i.e. cyberspace) into our contemporary society. The second part is referring to the promotion of political and social inclusion, something in which the emergence of e-government has a very large role. Something the EU Strategy points out as well, is that fundamental rights, democracy and the rule of law have to be protected in cyberspace, and that governments have a significant role in this (European Commission, 2013). This is especially important, because there is a significant increase in cybercrime and cyber-attacks over the last few years (European Commission, 2013; Europol, 2018; Patyal, Sampalli & Rahman, 2017). Aside from this increase in cyber threats, there has also been a shift from the targeting of individuals, towards the targeting of (large) companies, healthcare organisations and other public infrastructure (Europol, 2018; Patyal, Sampalli & Rahman, 2017). The cyber-attacks that hit the Ukrainian power grid in 2015 and the British National Health Service and other governmental digital infrastructure in 2017 are worrying examples of these recent developments. These cyber threats are undermining salient objectives which the United Nations have set in UN General Assembly Resolution 66/288, entitled “The Future We Want”: democracy, good governance and the rule of law at national and international levels (United Nations, 2019a). These objectives are essential for achieving sustainable development, as set out in the 2030 Agenda for Sustainable Development (SDGs).

Next to this increase in cyber threats, the United Nations (UN) have reported a rapid growth of e-government over the past 17 years. Especially in the areas of health, education, the environment and decent work, the complexity of e-government in promoting accountable, effective, inclusive, transparent and trustworthy public services is increasing significantly (United Nations, 2018). All these services require guaranteed continuity, but might also process people's privacy-sensitive data. Therefore, these services stand in need of robust digital platforms that are resilient to cyber-threats, which makes cybersecurity a key factor in the transformation to resilient e-government (United Nations, 2018).

Increasing the knowledge about the (characteristics of) the relationship between cybersecurity and e-government is important to foster and enable governments to invest in creating cyber-resilient digital public services. This study will contribute to that knowledge.

1.4.2 Scientific relevance

The phenomena of cybersecurity and e-government are both relatively young, as they only emerged after, and as a result of, the technological developments in Information and Communication Technologies (ICTs), the last three decades. This means that there is no extensive existing body of literature and theory on both concepts separately, let alone on the relationship between them. Several studies do investigate both cybersecurity and e-government, but not as two factors in relation to each other (Alharbi, Papadaki & Dowland, 2017; Botchwey, 2018; Li & Liao, 2018). These studies look at the cybersecurity *of* e-government development, instead of investigating both terms as separate phenomena that potentially have a relationship with each other. There are studies, however, that do look at the relationship between the two factors, but most of them do that from a very different perspective, in a very specific focus area or with a much smaller scope compared to this study. Zhang, Tang and Jayakar (2018), for instance, who approach the relationship from a more legislative perspective by using a socio-technical framework to examine the impact of the 2016 cybersecurity law in China on the e-government services in that country., therefore focussing solely on one country

The absence of a high amount of studies that provide an international comparison regarding the relationship between cybersecurity and e-government development indicates that there is a gap on this topic within the literature. Nevertheless, there are two main studies that *do* fall within this category (Onumo, Cullen & Ullah-Awan, 2017; Verkijika & De Wet, 2016). There are however, three main limitations within these studies, which are addressed in this study. Firstly, the limited scope. While the study by Onumo, Cullen and Ullah-Awan (2017) is a global comparison, the study by Verkijika and De Wet only includes 49 countries, which are all Sub-Saharan African countries. This means that their scope is limited quantity and variety. Secondly, there is no scientific consensus regarding the shape of the relationship between cybersecurity and e-government. Verkijika and De Wet (2016) conceptualise cybersecurity as an independent variable and e-government development as the dependent variable, while in the study by Onumo, Cullen and Ullah-Awan (2017), this is the other way around, expecting e-government development as independent variable to have an impact on cybersecurity as a dependent variable. Thirdly, neither of both studies investigate the separate components of cybersecurity and their individual relationships with e-government development. Hence, this study adds to the body of literature by having a wide scope, by adding to the scientific debate on the nature of the relationship and by providing insight in whether the difference in e-government development around the world can be explained by cybersecurity and more specifically, the separate parts of cybersecurity.

1.5 Thesis guide

In chapter 1, the background of this topic is discussed, as well as a brief consideration of previously conducted research and their findings. This consideration resulted in the formation of the main research question as well as the sub-questions. Chapter 2 will elaborate extensively on the concepts of 'cybersecurity' and 'e-government development' and therefore answer sub-question 1. Subsequently, chapter 3 will answer sub-question 2, by discussing the theoretical relationship between cybersecurity and e-government development. Here, the theoretical hypotheses, as well as the conceptual model will also be presented. Chapter 4 will then elaborate on the design of this research and the methods that are used for data collection and analysis. Here, sub-questions 3 and 4 will also be answered by presenting the descriptive statistics. Within chapter five, the results of the conducted pooled OLS regression analysis will be presented. The analysis and discussion of these results will take place in chapter 6, hence answering sub-question 5. Lastly, chapter 7 will answer the main research question of this study, and give some concluding statements.

2 Concepts: definitions, backgrounds and literature review

In this chapter, the first sub-question of this study will be answered: *what does the literature say about the concepts 'e-government development' and 'cybersecurity'?* First, both variables will be described in terms of definition and history. Discussing the definition(s) and preceding history of the concepts is necessary to be able to provide clarity on what exactly is meant with these initially ambiguous phenomena. Subsequently, this chapter provides a literature review regarding both concepts, in which previously found antecedents and outcomes will be discussed. Paragraph 2.1 will elaborate on e-government development, after which paragraph 2.2 will cover cybersecurity.

2.1 E-government development

2.1.1 Defining e-government

One of the earliest mentions of e-government can be found in a strategic document from 1993, on reengineering government through information technology, by then president of the United States, Bill Clinton (Lips & Shupann, 2009).

> *The government must not apply information technology haphazardly or sporadically. It also should not simply automate existing practices. Instead, public officials should view information technology as the essential infrastructure for government of the 21st Century, a modernized 'electronic government' to give citizens broader, more timely access to information and services through efficient, customer- responsive processes.*
>
> US Government (under Clinton administration) (1993: p.1)

Since the technological development of these information and communication technologies (ICTs) have made this reengineering of government possible, electronic government, or e-government, has emerged as a popular catch phrase in public administration (Yildiz, 2007). This, because the newly emerged technologies were believed to have tremendous administrative potential. Nevertheless, there is not any universally accepted definition of the concept of e-government (Halchin, 2004). In 2002, the United Nations together with the American Society for Public Administration (ASPA) defined e-government as "utilising the Internet and the

World-Wide-Web for delivering government information and service to citizens" (UN & ASPA, 2002: p. 1). However, this definition is rather limited, especially in terms of the recipients of e-government. Other definitions expand more, by describing e-government as the usage of information technology to deliver government services to the customers (and suppliers) of governments (Means & Schneider, 2000). These customers are then most often categorised in three groups: citizens, businesses and other governments. Brown and Brudney (2001) as well as Homburg and Bekkers (2004) also use this categorisation, by dividing e-government services up in three forms: government-to-citizen (G2C), government-to-business (G2B) and government-to-government (G2G). They, however, include another dimension into the definition, by stating that e-government should have as a goal to enhance the efficiency of governmental service delivery. With this, Brown and Brudney (2001) and Homburg and Bekkers (2004) point to a direct positive effect e-government can have. Other authors have also indicated positive implications for the governmental use of ICTs, such as improved service delivery (Bekkers & Zouridis, 1999), efficiency and effectiveness (Heeks, 2001), decentralisation and transparency (La Porte, De Jong & Demchak, 1999) and accountability (Ghere & Young, 1998; Heeks 1998; McGregor, 2001). The World Bank (2001) combined all the aforementioned elements into one, what seems to be the most complete, definition for e-government:

> *Government-owned or operated systems of information and communications technologies (ICTs) that transform relations with citizens, the private sector and/or other government agencies so as to promote citizen empowerment, improve service delivery, strengthen accountability, increase transparency, or improve government efficiency.*
>
> World Bank, 2001

The United Nations uses an almost exactly similar definition of e-government, describing it as the application of ICT in government operations, achieving public ends by digital means (United Nations, 2019b). Every two years, the United Nations conducts a survey research, and publishes a report on the state of e-government development of its member states: the E-Government Development Index (EGDI). The UN does not only consider a country's creation of electronic government services as important component of e-government, but also the e-government readiness of a country. Because of this, the UN defines (and uses for its index) three important dimensions of e-government: provision of online services, measured by the Online Service Index (OSI); telecommunication connectivity, measured by the Telecommunications Infrastructure

Index (TII); and human capacity, measured by the Human Capital Index (HCI) (United Nations, 2019c).

2.1.2 E-government as the result of New Public Management (NPM)

As shortly touched upon in the first chapter, public administration discourse and dominant public administration theories have significantly evolved over the last decades. In general, public administration denotes "the institutions of public bureaucracy within a state, the organizational structures which form the basis of public decision-making and implementation; and the arrangements by which public services are delivered" (Bradbury, 2009).

2.1.2.1 NPM as predecessor for e-government

From the end of the 1970s,public administration in Western world appeared to move itself into a new era, an era of administrative reforms, diverting away from the traditional model of bureaucracy which was mainly inspired by Max Weber's work (Hughes, 2003). In the United States, Western Europe, but also in Australia and New Zealand, managerial reforms took place within the public sector and 'New Public Management' (NPM) was born (Kickert, 1997). This new trend within public administration has the same core characteristics everywhere it appears: it introduces ideas, models and techniques that are used in the private sector, into the public sector. These mainly consist of business management techniques, greater service and client orientation, the introduction of market mechanisms and competition in public administrations (Boyne, 2002; Kickert, 1997). The main reason for these reforms was economic-financial. After the oil crisis of the 1970s, a vast number of governments ended up with high public deficits, and the traditional extensive welfare state became unaffordable. This forced the public sector to move towards more efficient ways of conduct (Kickert, 1997). There are many similarities in functions and objectives, between the concepts of NPM and e-government (Torres, Pina & Royo, 2005).

According to various scholars, the most recent development in public administration discourse is New Public Governance (NPG). Where NPM is mainly rooted in economic/market and managerial theory, NPG is more based on organisational sociology and network theory, representing the highly fragmented environment of public managers and public organisations in the twenty-first century (Osborne, 2006). NPG theory describes a system in which multiple inter-dependent actors contribute to the delivery of public services and in which multiple processes inform the policy making process, instead of outputs as in NPM (Osbourne, 2006). In other words, NPG can be seen as the blurring of boundaries between the public sector, private sector and civil society, which are collectively responsible for tackling social and economic matters (Ewalt, 2001). The emergence of NPG also influences e-government. According to many scholars, there is a transition from 'e-government' to 'e-governance' (Berce, Lanfranco & Vehovar, 2008; Orelli, Padovani & del Sordo, 2013). E-governance differs from e-government, by focusing on the use of ICTs not only to deliver public services, but to foster participation and democracy in society, and create this collective participation and responsibility as NPG describes (Berce, Lanfranco & Vehovar, 2008). However, NPG and e-governance fall outside of the scope of this research. The main reason for this is that the UN assesses e-governance aspects (e-democracy and e-participation) of countries by use of another index: the UN E-participation index. This study will only make use of the EGDI and will therefore not focus on e-governance and NPG.

2.1.2.3 NPM and e-government

The emergence of e-government in the last 2 decades, can be seen as an extension of New Public Management (NPM) by making use of newly developed ICT technologies. Many of the characteristics of e-government are inherited from NPM inspired reforms (Torres, Pina & Royo, 2005). Examples of this are better delivery of government services to citizens; improved interactions with businesses and industry; citizen empowerment through access to information; and more efficient government management (Homburg & Bekkers, 2004). These characteristics were aimed to result in benefits such as less corruption, increased transparency, revenue growth and/or cost reductions (Homburg & Bekkers, 2004). Again, traits that very much resemble the private sector-based/managerial essence of NPM, described by Hood (1991) and Kickert (1997). Nevertheless, there are also some internal inconsistencies when merging e-government one on one with NPM. The most important example of this are the relatively high costs of a transition to e-government (Homburg & Bekkers, 2004). Nonetheless, this is the case for most managerial and governmental reforms, and does negate the reduced costs of a functioning e-government.

2.1.3 Literature review

For e-government, a systematic bibliographic search was performed, using Web of Science. The search terms for this bibliographic search were "e-government" AND "development". Subsequently, the bibliography of the found papers were examined for additional relevant sources. Table 1 provides an overview of the approach and criteria for the bibliographic search.

Table 1 | Bibliographic search on e-government

Web of Science search	Search terms: "e-government" AND "development"
Inclusion criteria	Sources providing a definition of e-government Sources describing the history/origins of e-government Sources describing antecedents of e-government Sources describing outcomes of e-government
Exclusion criteria	Sources describing e-governance Sources not in English Sources not accessible through open access or EUR subscription
Manual search for additional literature	Bibliography of the initially found literature Manual searches on UN and World Bank websites

This bibliographic search resulted in a total amount of 49 sources, of which 44 are academic sources (peer reviewed articles in journals or books) and 5 are grey literature, coming from international organisations or governmental institutions. Many sources, especially for the definition and history of e-government, resulted out of the examination of the reference lists of the initially found literature.

The literature review provides insight into the factors that act as antecedents and consequences for the phenomenon of e-government development. Insight in these factors is necessary to determine the starting point of the research and presenting the preceding research into the phenomenon which has shaped the landscape in which this research falls.

2.1.3.1 Antecedents

When investigating the antecedents for e-government, one has to be wary of the difference of perspective of (the introduction/adoption of) e-government from the government's side and (the adoption/usage of) e-government on the end user's side. There are many studies that look at antecedents for citizens' adoption and usage of e-government services, such as gender, age, social position and income (Bélanger & Carter, 2009; Chourdie & Dwivedi, 2005; Colesca & Dobrica, 2008; Reddick, 2005; Taipale, 2013; Van Dijk, Pieterson, Van Deuren & Ebbers, 2007). This study, however, does not take on the citizens' perspective, but looks at e-government from the public management side. As some authors state that e-government is a direct result of NPM (Torres, Pina & Royo, 2005) or that the two are at least mutually reinforcing (Homburg & Bekkers, 2004), one could claim that New Public Management is an important antecedent for the adoption and development of e-government in public administration.

A study by Kabanov and Sungurov (2016) has looked at different political, technological, socio-economic and administrative factors and the significance of their influence on the development of e-government in various Russian regions. They have found that 'democratic political regime', 'technological advancement', 'effectiveness of bureaucracy' and 'ICT investment' are key predictors for the maturity of e-government. The study by Kabanov and Sungurov (2016) takes a government-centric approach. Sorn-In, Tuamsuk and Chaopanon (2015) on the other hand, take on a citizen-centric approach and found that from the viewpoints of citizens and public sector servants, five factors affect the development of e-government: e-government services quality, economy and society, policy and governance, information technology infrastructure and organisation (Sorn-In, Tuamsuk, & Chaopanon, 2015). Arduini et al. (2013) find a comparable set of factors that have a role in the development of e-government, in the context of Italian municipalities. They state that various technological, organisational and contextual factors all have an influence on the development of e-government and that public administrations need to take on a holistic approach, encompassing factors of all these three types, to be able to develop e-government services in an effective and efficient manner (Arduini et al., 2013).

Another interesting factor is corruption. Many studies are focused on the factor corruption being decreased by the emergence of e-government, therefore being a consequence/outcome (see next sub-paragraph). However, Khan and Krishnan (2019) conceptualise corruption as a possible influencing factor on e-government maturity, deeming corruption as an antecedent for (the maturity of) e-government. The authors present a conceptual model based on 5 key theoretical perspectives, in which they link corruption with e-government maturity, with corruption as the antecedent for e-government maturity. Aladwani (2016) also found that corruption is a deciding factor for the success of e-government projects. He concluded that corruption in developing societies can restrict moral and governance capabilities of administrative bodies, overseeing e-government systems, leading to ill development and effectiveness of these systems (Aladwani, 2016). Verkijika and De Wet (2016) also consider corruption as an important factor having an influence on the development of e-government. Besides corruption, they investigate five other factors of which they expect have an influence on the development of e-government: national income, gender equality, population age, innovation and cybersecurity. For all six variables they investigate, they find a positive relationship with the development of e-government (Verkijika & De Wet, 2016).

2.1.3.2 Consequences

Across the antecedents of e-government, there are the consequences. As mentioned before, e-government was originally aimed to reach objectives such as better public service delivery, less corruption, more transparency and increased cost efficiency (Bekkers, 2003; Homburg & Bekkers, 2004; Lips & Schuppan, 2009; Torres, Pina & Royo, 2005). A study by Máchová, Volejníková and Lněnička (2018) that looked at the relationship between the development of e-government and levels of corruption in the context of economic perspective showed that there is indeed a positive relationship between the two factors, concluding that increased development of e-government leads to lower levels of corruption. Studies by Garcia-Murillo and Otega (2010) and by Lupu and Lazăr (2015) have found the same effect of e-government development on levels of corruption, on a large international scale. Several other studies found similar results, but with slight nuances: the effect is stronger in developing countries compared to developed countries (Mistry & Jalal, 2012); e-government development leads to decreased corruption mainly in the areas of taxes and government contracts (Bhatnagar, 2003; Shim & Eom, 2008); e-government decreases corruption through enhancing the effectiveness of internal control and management of corrupt behaviour by promoting government transparency and accountability (Shim & Eom, 2008); and national culture has a moderating effect on the relationship between e-government and levels of corruption (Nam, 2018).

West (2004) has investigated what influence the development of e-government has on three factors: public service delivery, democratic responsiveness and public attitudes. This study, which was conducted in the United States of America, has found that the development of e-government has the possibility of enhancing the democratic responsiveness and the public belief that the government is effective. Besides this, West (2004) argues that there is definitely a changed and improved public service delivery, but not nearly as much as there could be, looking at the potential of the e-government revolution.

Research by Lee (2017) found that the development of e-government has an effect on environmental sustainability in Small Island Developing States (SIDS), in multiple ways. Based on a quantitative analysis of a panel dataset, the author found that the development of e-government has a direct effect on environmental sustainability, but also an indirect effect, through government effectiveness as a mediating factor (Lee, 2017).

2.1.3.3 Reciprocal relationships

Several studies investigate the relationship between e-government and the digital economy (Ali, Hoque, & Alam, 2018; Zhao, Wallis & Singh, 2015). Both studies have found a strong positive reciprocal relationship between e-government and the digital economy. This means that an increased digitalisation of the economy (as antecedent) can drive e-government, but also the other way around (Zhao, Wallis & Singh, 2015). This reversed relationship deems the digital economy as a consequence of e-government as well. Both studies have addressed this reciprocal relationship in a multidimensional way and found that social, economic, political, legal, technological, demographical and certain national cultural characteristics have significant effects on e-government and the digital economy (Ali, Hoque & Alam, 2018).

A study by Wallis & Zhao (2018) found a reciprocal relationship involving e-government as well. They state that there is a two-way relationship between e-government and government effectiveness. This relationship can, according to the authors, be explained by the path dependent nature of trust development in public servants (Wallis & Zhao, 2018).

To conclude, and answer this study's first sub-question, e-government entails the use of ICTs for the provision of public services, originated from NPM traits (such as (cost) efficiency) and made possible by technological advancement. Factors such as corruption, innovation, cybersecurity, national income, and various other socio-economic factors can be categorised as influencing e-government development (antecedents). On the other hand, according to many scholars, e-government improves public service delivery effectiveness, efficiency and public transparency. These, as well as factors such as corruption, democratic responsiveness and even environmental sustainability are outcomes of e-government. There are two phenomena, with which according to some studies, e-government has a reciprocal relationship: government effectiveness and the digital economy.

2.2 Cybersecurity

2.2.1 Defining cybersecurity

The concept of 'cybersecurity' is an ambiguous term, although it becomes more clear what it entails when breaking it down to 'cyber' and 'security'. 'Security', as stated by Baldwin (1997: p. 13), is the "low probability of damage to acquired values". An ideal state of security would be the complete absence of threats (Wolfers, 1952). However, since this is an utopian idea, the definition by Baldwin (1997) is a much more workable phraseology. ‘Cyberspace’, as defined by the US Department of Defense, entails “a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (Gortney, 2016: p. 5). Thus, cybersecurity entails the low probability of damage to acquired values in this global domain, called ‘cyberspace’. In most literature however, cybersecurity is used as an all-inclusive term, serving as terminology for many (slightly to highly) varying constructs (Von Solms & van Niekerk, 2013). According to Goodman and Lin (eds.) (2007: p. 154), cybersecurity “concerns with the understanding of surrounding issues of diverse cyber-attacks and devising defence strategies (i.e., countermeasures) that preserve confidentiality, integrity and availability of any digital and information technologies”. The protection of confidentiality, integrity and availability of technologies is something which is often reoccurring in the literature on cybersecurity. Jang-Jaccard and Nepal (2014: p. 974) describe these terms as follows:

- **Confidentiality** is referred to as the prevention of the disclosure of any information, to unauthorized entities
- **Integrity** is referred to as the prevention of the modification or deletion of information in any unauthorized manner or by any unauthorized entity
- **Availability** is referred to as the reassurance that systems that deliver, process and store information are continuously accessible for their authorized users

The interplay of these three terms (also known as CIA), and the protection of them in the context of the cyber domain, is also often in governmental strategies on cybersecurity. One example is the 2013 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, which defines cybersecurity as follows (European Commission, 2013: p. 3):

> *Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.*

Von Solms and Van Niekerk (2013) advocate for a precise phraseology, pointing out the difference between ‘information security’ and ‘cybersecurity’. The CIA abbreviation should be categorised as ‘information security’, because confidentiality, integrity and availability are characteristics that are connected to information and therefore the protection of these characteristics inherently too (Von Solms & van Niekerk, 2013). ‘Cybersecurity’ on the other hand, is a concept that comprises a wider range of phenomena. Von Solms and Van Niekerk (2013) consider a ‘information security’ a type of ‘cybersecurity’, along with several phenomena that involve the protection of an entity’s non-information based assets from risks stemming from interaction with cyberspace. The authors move beyond the conception of mere technology and describe e.g. cyber-bullying, the Internet of Things and cyber-terrorism as examples of phenomena that do not fall under ‘information security’ (no breach of CIA), but do fall under ‘cybersecurity’ (Von Solms & van Niekerk, 2013). Some scholars go even further than that, stating that cybersecurity research and discourse tends to over-emphasize the ‘cyber’ in cybersecurity, leaving the human security concerns underexposed (Ashenden, Coles-Kemp & O’Hara, 2018; Salminen & Hossain, 2018). As mentioned in the preceding paragraph, recent cybersecurity strategies have shown a shift to more encompassing perceptions of cybersecurity, demonstrating a more holistic approach to the problem.

The International Telecommunications Unit (ITU) also takes on this holistic approach, and distinguish five pillars, that shape the inherent building blocks of a national cybersecurity culture (ITU, 2018):

- Legal;
- Technical;
- Organisational;
- Capacity-building and;
- Cooperation.

Legal measures, entailing legislation, regulation and enforcement, allow a country to determine and shape the judicial framework concerning entities and activities in the cyber realm. It provides the state with authority to investigate and where needed, prosecute crimes and impose sanctions. Moreover, the legal framework is the basis with which regional, national and international practices can be harmonized and international cooperation in the field of cybersecurity can be established (ITU, 2018).

As mentioned, the technical aspect is the most basic and conventional building block when thinking about cybersecurity. Every country has to possess the right technical skills and IT systems to be able to timely detect and respond to cyber threats (ITU, 2018). Therefore, the technological side of cybersecurity, rooted in ICT developments, is a vital part of a country's cybersecurity development, and an antecedent for cybersecurity in general.

Organisational measures, of which national cybersecurity strategies themselves are an important example, are needed to successfully implement any cybersecurity aspiration. Important components of this are clearly set objectives and national agencies and organisations that are being established and enabled with the mandate and the resources to be able to achieve these objectives. They need to implement the cybersecurity strategies as well as evaluate the outcomes (ITU, 2018).

Capacity-building, inherently connected to the first three building blocks, entails the creation of public awareness, the education an certification of cybersecurity professionals and trainings, courses and academia in the field of cybersecurity knowledge and practices (ITU, 2018). This essential building block is the reflection of the 'doctrine of public cybersecurity' by Mulligan and Schneider (2011) (see paragraph 2.2.2) as it emphasizes the socio-economic and political implications of cybersecurity by fostering human and institutional capacity building.

Cyber-related threats are completely temporally and spatially independent, meaning that they can emerge quickly at any moment, not taking national or physical borders into account. This means that for cybersecurity, a multi-stakeholder and multi-national approach is needed. Different types of cooperation, such as multi- and bilateral agreements, public-private partnerships and inter-agency cooperation, strengthen the cyber capabilities in order to adequately respond to cyber threats (ITU, 2018).

Within the debate on the definition on cybersecurity, this study conceptualises cybersecurity in the broad sense of the word, not limited to information security, hereby following the definition of the ITU as much as possible. As mentioned, the ITU takes on a holistic approach towards the concept of cybersecurity, as it includes a wide array of components, going much broader than mere information security, i.e. confidentiality, integrity and availability of information.

2.2.2 History: from tech-tool to total dependency

By the end of the 20th century, the world has seen a 'communications revolution' or 'information revolution'. The Internet was 'founded' in the 1960s, but it only became of interest for governments and part of the public administration discourse in the 1990s, when the Internet evolved into a large scale medium for the general public (Koops, 2011). By adopting universal binary code, almost any type of information can now be transported through time and space by the use of digital networks (Mayer-Schönberger & Hurley, 2000). This revolution, also called the 'digital revolution' has tremendous implications for all human life on earth. Nonetheless, it is also creating new threats and risks. With digital networks taking over an increasing amount of our daily activities, including industries, businesses, private life and governments, we simultaneously become increasingly dependent on these very digital networks (Mayer-Schönberger & Hurley, 2000). Today, the world economy is driven by big data, social networks, online transactions and information that is stored, managed and processed via the Internet and ICTs (Bendovschi, 2015). The dependency on these ICT-based activities brings about new risks and vulnerabilities (Bendovschi, 2015; Mayer-Schönberger & Hurley, 2000; Pupillo, 2018: Warner, 2012).

Previous doctrines on cybersecurity stem from the 20th century, and were focused on technology. Policymakers therefore sought technological solutions to combat the issue of cybersecurity and societal factors and values were largely ignored (Mulligan & Schneider, 2011). Mere technological solutions were not the way to solve the mere technological problems, and later cybersecurity doctrines involved a more all-encompassing way of looking at cybersecurity. Several authors talk about cybersecurity as being a 'public good' (Mulligan & Schneider, 2011; Stevens, 2018). Mulligan and Schneider (2011) therefore introduce the 'doctrine of public cybersecurity'. It being a public good means that cybersecurity is non-rivalrous (one's ability of enjoying it does not diminish another's) and non-excludable (ones who enjoy the benefits of it are not easily excluded from this). The authors compare the characteristics of cybersecurity with those of another well-known public good: public health (Mulligan and Schneider, 2011).

In today's society, the notion that cybersecurity is a public good, seems to be the general perception: governments' approach to cybersecurity is that society as a whole needs to be protected, not just individuals and organisations as distinct actors (OECD, 2012). National governments are developing and adopting cybersecurity strategies to address a growing amount of cyber-related threats such as state-led cyber-attacks against national infrastructure, criminals ransoming computer systems with commercial interest, hacktivists using computer systems to protest against activities of firms or organisations and identity thefts by cybercriminals (Sutherland, 2017). Generally, these kinds of threats and activities can be categorised as:

- cybercrime;

- cyberespionage;
- cyberterrorism; or
- cyberwarfare.

Cybersecurity strategies to adequately respond to these threats, have been developed, and are still being redeveloped at a fast pace, on local, national and international level. All these strategies have the same objective: assuring and increasing cyber resilience (Štitilis, Pakutinskas, & Malinauskaitė, 2017). According to the OECD's (2012) international comparative report on cybersecurity strategies, these strategies should all approach cybersecurity in an 'integrated and comprehensive manner', instead of the fragmented manner in which this issue was approached in the past. The main reason for this is the shift of the Internet as being merely 'useful' to society, to being 'essential' to it, much resembling Mulligan and Schneider's (2011) argumentation of cybersecurity as a public good. What then this holistic approach towards cybersecurity could entail is touched upon by Sutherland (2017). According to him, the adequate governance of cybersecurity entails the protection of data and coordination of cybersecurity activities across the whole of government, including sub-national levels (e.g. municipalities), independent agencies, and contractors. Moreover, governments must take an active role in influencing the cyber-related activities of businesses, households and individuals (Sutherland, 2017).

2.2.3 Literature review

For cybersecurity, a systematic bibliographic search was performed, using Web of Science. For this search, multiple combinations of search terms were used, because results of these were all considered relevant for this study and these terms are used interchangeably in (grey) literature: "cybersecurity"/"cyber-security"/"cyber security" AND "commitment" /"maturity"/"development". Commitment, maturity and development were added as search terms because it narrows the search down to (a country's) level of cybersecurity, instead of looking at the mere technical side of cybersecurity. These terms are also interchangeably used in the reports regarding the Global Cybersecurity Index, by the ITU (ITU, 2018; ITU, 2017; ITU, 2014). Subsequently, the bibliography of the found papers were examined for additional relevant sources. Table 1 provides an overview of the approach and criteria for the bibliographic search.

Table 2 | Bibliographic search on cybersecurity

Web of Science search	Search terms: “cybersecurity”/”cyber-security”/”cyber security” AND “commitment”/”maturity”/”development”
Inclusion criteria	Sources providing a definition of cybersecurity Sources describing the history/origins of cybersecurity Sources describing antecedents of cybersecurity Sources describing outcomes of cybersecurity
Exclusion criteria	Sources focusing on the private sector Sources focusing on purely technical aspects Sources not in English Sources not accessible through open access or EUR subscription
Manual search for additional literature	Bibliography of the initially found literature Manual searches on website of the ITU and EU

This bibliographic search resulted in a total amount of 25 used sources, of which 22 are academic sources (peer reviewed articles in journals or books) and 3 are grey literature, coming from international organisations or governmental institutions. Many sources, especially for the definition and history of cybersecurity, resulted out of the examination of the reference lists of the initially found literature.

2.2.3.1 Antecedents

Cybersecurity, as aforementioned, is a highly ambiguous term. According to Bambauer (2012), the quick rise as concept and practice has hindered definitional consensus on cybersecurity, meaning that there is no common agreement upon what cybersecurity exactly is and what it requires. Consequently, this means that determining antecedents and outcomes/consequences is also complex. Above anything else, cybersecurity is inextricably connected with, and contingent on the Internet. The existence of the Internet in turn, relies completely upon information and communication technologies (ICTs) (Stevens, 2018: p. 2). The chain of antecedents can be traced back all the way to the development of binary code and the first ever computer, explained in the previous paragraph. This is the most important path of antecedents, albeit approaching cybersecurity from a technological perspective.

Various scholars emphasize the socio-economic, social and human dimension to cybersecurity as important counterbalance against the technical dimension (Ashenden, Coles-Kemp & O’Hara, 2018; Salminen & Hossain, 2018; Stevens, 2018). Where theories on security often focus on the interdisciplinary relationships between economy, technology, politics and social aspects in society, cybersecurity policy and its implications are mostly directed at the technical and/or physical protection of the digital infrastructure (Ashenden, Coles-Kemp & O'Hara, 2018).

2.2.3.2 Consequences

With the digital revolution came the emergence of the Internet and the cyber realm, resulting in a new paradigm for our contemporary society: the network society (Webster, 2014). This has led to digital globalisation, as digital information is not limited by temporal and spatial restrictions (Park, 2016). Data can be transported, to virtually any location on the globe, at any point in time (Warner, 2012; Jang-Jaccard & Nepal, 2014; Webster, 2014). Cybersecurity is a response to the threats this new technological advancement brings along. Contrary to the temporally and spatially independent nature of cyber-threats, cybersecurity is most often organised and implemented on a national level. Therefore there are consequential factors related to a country's commitment to, and maturity of cybersecurity. Kshetri (2016) states that the poor cybersecurity orientation by the government in India plays a large role in the booming prevalence of cyber-crimes and cyber threats in that country. According to him, "cybercriminals consider Indian computers as low hanging fruit due to weak cybersecurity (Kshetri, 2016). The reasons for this, in the Indian case, lay in factors (low level of human development, underdeveloped technical skills and systems, lack of resources and organisation) that are very much connected to the five pillars as building blocks for solid, holistic cybersecurity development, explained in the previous sub-paragraph. In short, it means that a low level of cybersecurity in a country leads to an increased victimisation of individuals, businesses and governments in that country, reinforcing the low level of cybersecurity. An interesting paradox in this causality however, is that the Indian law enforcement agencies' unsupportive attitudes and unwillingness to help victims have contributed to a low reporting rate of cybercrime cases (Kshetri, 2016).

To conclude, and answer this study's second sub-question, cybersecurity is a highly ambiguous phenomenon, often revolving around confidentiality, integrity and availability of data (information security). As technological advancement created the cyber realm, cyber-threats emerged which asked for cybersecurity efforts by (national) governments. The cybersecurity of countries, as focused on in this study, has five main characteristics: legal, technical, organisational, capacity-building and cooperation. Many technical, but also socio-economic factors can be perceived an antecedent for the versatile concept of cybersecurity. As for outcomes, the degree of national cybersecurity can influence cyber-threats elsewhere, due to the space- and time-independent nature of these threats.

3 Theoretical framework

This chapter will answer the second sub-question: *what is, according to the literature, the theoretical relationship between cybersecurity and e-government?* In paragraph 3.1, a more general and broad theoretical underpinning of the concepts security and development will be introduced, as well as their relatedness. Paragraph 3.2 expands on this relationship, but from the digital perspective. Paragraph 3.3 contains the hypotheses and conceptual model of this research, with which the research question will be empirically tested.

3.1 Security and development

"Humanity will not enjoy development without security and will not enjoy security without development and will not enjoy either without respect for human rights."

Former UN Secretary-General Kofi Annan, cited in UN General Assembly 2005 (p. 6)

As stated by former UN Secretary-General Kofi Annan, security and development are inextricably connected, meaning that there is a strong relationship between these two broad concepts. In the disciplines of international relations (IR) and development, this relationship between security and development is endorsed, as showed in works by for instance Chandler (2007), Duffield (2010), Stern and Öjendal (2010), and Stewart (2005). In security strategies and policy development, this relationship has gained popularity as well, as can be seen in the following phrase of the 2009 EU Security Strategy (ESS): "as the ESS and the 2005 Consensus on Development have acknowledged, there cannot be sustainable development without peace and security, and without development and poverty eradication there will be no sustainable peace" (Council of the European Union, 2008: p. 8). Moreover, UN agencies such as the UN Development Programme (UNDP) and the Department of Peacekeeping Operations (DPKO) increasingly take the connection between security and development into consideration when planning international conflict- and development programmes (International Peace Academy, 2004).

Even though the existence and importance of the relationship between security and development is acknowledged from both a policy standpoint (UN, EU, International Peace Academy) as well as from an academic standpoint (Ball & Halevy, 1996; Kapila & Wermester, 2002; Slater, 2008), the assumptions behind this relationship are based on very little empirical evidence (Chandler, 2007). In the discipline of international relations and development — with which the relationship between these two concepts has mainly been analysed until now — this relationship can perhaps better be seen as '*potentially* mutually reinforcing goals', as it does not automatically apply to policy arenas within this discipline (prevention, state-building, peace-building) (Chandler, 2007). For this reason, it might be interesting to look at the relationship between security and development with a different pair of glasses and apply this relationship in an entirely different context: the digital realm.

3.2 The digital relationship between security and development

As described in chapter 2, the world has entered into the digital age over the last decades, and has seen the emergence of the digital (or cyber-) realm, offering a wide array of new possibilities and risks (Karake-Shalhoub & Al Qasimi, 2010). Various previous cyber-attacks (such as on a Ukrainian power grid in 2015 and on the British National Health Service in 2017) have shown how cyber threats can affect critical infrastructures. For governments, this has played an important role in perceiving 'cybersecurity' as an increasingly important area within 'security' (Von Solms & van Niekerk, 2013). According to international relations and security literature, the cyber realm is the fifth domain of war and security, after land, sea, air and space (Bayraktar, 2014). On the other hand, the emergence of the digital economy (e-economy) and the digital divide within society, have put digital development in the centre of attention when it comes to socio-economic and development-related issues (Webster, 2014). For governments, the digitalisation of public services plays a central role in this digital development as they cannot lag behind in an increasingly digitalising society. An implication of these recent developments regarding the concepts of 'security' and 'development' is therefore to re-examine their relationship, but then from a digital point of view. For this reason, this study extrapolates the general concepts of 'security' and 'development', to respectively 'cybersecurity' and 'e-government development'. There are many studies that proclaim a relationship between the concepts of e-government development and either cybersecurity as a whole (Onumo, Cullen & Ullah-Awan, 2017; Verkijika & De Wet, 2016) or components of cybersecurity (Alharbi, Papadaki & Dowland, 2017; Burn & Robins, 2003; Conklin, 2007; Ebrahim & Irani, 2005; Khanyako & Maiga, 2013; Lenk & Traunmuller, 2000; Li & Stevenson, 2002; Ndou, 2004; Norris, Fletcher & Holden, 2001; Sarrayrih and Sriram, 2015; Zhang, Tang & Jayakar, 2018).

According to Baker (2014), cybersecurity is critical for development. More specifically, she describes that focusing on cybercrime, cyberterrorism and cyberwarfare, by using cybersecurity capacity building, can bolster a country's socio-economic development (Baker, 2014). Based on empirical research done within Pakistan and India, Baker (2014) introduced a conceptual model in which cybersecurity, consisting of several components (internal governance, private sector partners, active cyber-citizenry and foreign government relations) has a positive influence on socio-economic development of developing countries. Part of this socio-economic development is the rapid development of the digital society, embodied in new phenomena such as e-commerce and e-government (Karake-Shalhoub & Al Qasimi, 2010). Verkijika and De Wet (2016) have explored this relationship between cybersecurity and e-government development. Their assumption is that digital security threats related to privacy, identity and data systems significantly affect citizens' trust in e-government systems. Hence, a higher level of cybersecurity will increase people's willingness to adopt e-government, which in turn leads to increased development of e-government (Khanyako & Maiga, 2013; Verkijika & De Wet, 2016). This crucial importance of cybersecurity for the adoption and development of e-government services is also recognized by international organisations (ITU, 2018; United Nations, 2018). These are also the organisations which investigate the level of cybersecurity (ITU) and e-government development (United Nations) on a global scale, and publish biannual reports and indexes on these phenomena. As Baker (2014) used several components of cybersecurity perceived to be vital for socio-economic development, the United Nations (2018) perceives five pillars, encompassing cybersecurity, as vital components that lay a solid foundation for the creation of a secure e-government system: legal, technical, organisational, capacity-building and cooperation. These pillars for cybersecurity are not made up by the UN itself, but are the five pillars along which the International Telecommunications Union (ITU) measures the level of cybersecurity of its member states, and on which the Global Cybersecurity Index (GCI) is based.

The section below touches upon the theoretical relationship between each individual pillar of cybersecurity on the one hand and the development of e-government on the other hand, on which the subsequently introduced hypotheses are based.

Legal

The legal framework is the starting point which allows governments to define basic response mechanisms to cyber-attacks, including within e-government systems (United Nations, 2018). In the age of digital globalisation, where countries engage more and more in e-commerce and e-government, the largest stumbling blocks for this digital development according to Karake-Shalhoub and Al Qasimi (2010) are a) the absence of regulation and legislation protecting consumers, intellectual property, personal data, information systems and networks, and b) the absence/inadequacy of laws dealing with cybercrimes. A study by Zhang, Tang and Jayakar (2018), which specifically investigated the impact of a Chinese cybersecurity law on e-government, found that cybersecurity legislation positively influences the willingness to utilize e-government, through mediating factors such as trust. Another study, conducted by Alharbi, Papadaki and Dowland (2017) also found that the development and adoption of e-government services is contingent upon cybersecurity legislation. Considering the above, the first hypothesis of this study comprises the following: the 'legal' component of cybersecurity has a positive relationship with the development of e-government.

Technical

Without solid technical measures, such as public and private sector Computer Incident Response Teams (CIRTs), countries remain digitally vulnerable, which makes technology the primary frontier of defence against cyber threats (ITU, 2018). The establishment of a resilient digital infrastructure is therefore a prerequisite for successful e-government development (United Nations, 2018). Verkijika and De Wet (2016) have found that technological innovation in a country positively influences e-government development. Nevertheless, technological innovation does not automatically indicate technology for cybersecurity purposes. The technical component of cybersecurity is the one that is most related with the least 'human' factor of cybersecurity: information security, as described by Jang-Jaccard and Nepal (2014) as confidentiality, integrity and confidentiality of data (see paragraph 2.2.1). Information security is an essential ingredient for the development and adoption for e-government technology (Khanyako & Maiga, 2013). Several studies have confirmed this relationship, both qualitative (Conklin, 2007) and quantitative (Khanyako & Maiga, 2013). Considering the above, the second hypothesis of this study comprises the following: the 'technical' component of cybersecurity has a positive relationship with the development of e-government.

Organisational

Away from the technical factor, into the strategic and policy factor of cybersecurity, the organisational component focuses more on the existence of cybersecurity strategies, national cyber agencies and cybersecurity metrics (ITU, 2018), and perceives this as a third vital component for the development of e-government (United Nations, 2018). Several studies have investigated the relationship between organisational factors and the development and adoption of e-government. Ebrahim and Irani (2005) describe the 'organisational barrier' as one of the most important potential obstacles for the development, implementation and adoption of e-government. Within this organisational barrier, several other studies highlight the importance of different organisational factors, such as strategy (Lenk & Traunmuller, 2000; Li & Stevenson, 2002) and well-functioning and communicating governmental institutions (Burn and Robins, 2003). Considering the above, the third hypothesis of this study comprises the following: the 'organisational' component of cybersecurity has a positive relationship with the development of e-government.

Capacity-building

Capacity building relates very much to the non-technical part of cybersecurity, and is intrinsic to the first three pillars of cybersecurity (ITU, 2018). Building knowledge, understanding and awareness concerning cybersecurity, are essential parts in a country's development (Muller, 2015). Without this awareness and adequate education, that result in IT know-how, skills and cyber-hygiene, securing technological systems, including e-government systems, is rendered inefficient, if not useless (Tamarkin, 2015).This cybersecurity capacity building also plays an important role in the adoption and development of e-government services, as Ebrahim and Irani (2005) point out. Heeks (2001) calls this prerequisite the 'human infrastructure'. In a USA-based research by the International City/Country Management Association and Public Technology Inc., the lack of well-educated and skilful IT and cybersecurity professionals is found as the number one barrier for e-government (Norris, Fletcher & Holden, 2001). A more recent study, by Sarrayrih and Sriram (2015), showed that removing data- and information security concerns from people's minds by training and educating the public in using ICT resources is a requirement for the successful development of e-government. Considering the above, the fourth hypothesis of this study comprises the following: the 'capacity-building' component of cybersecurity has a positive relationship with the development of e-government.

Cooperation

The last important component of cybersecurity which, based on the theory and previous studies, has a relationship with e-government development, is cooperation. Given the interconnectedness of data and digital systems, ensuring cybersecurity requires the input of and cooperation of all sectors and disciplines (ITU, 2018). Constant dialogue and sharing of best practices is imperative for the creation of sufficient cybersecurity capabilities to be able to defend against and respond to cyber threats. This cooperation at the intergovernmental level, among agencies at the national level, and with the private sector, civil society and academia, will enhance the cybersecurity of e-government systems. E-government systems cannot be developed and operated securely and effectively without the collaboration between and within these organisational structures (United Nations, 2018). Research by Ndou (2004) confirms this by categorising partnership and collaboration at local, regional and national level, as well as between public and private actors as one of the main challenges for a successful implementation of e-government. Considering the above, the fifth hypothesis of this study comprises the following: the 'cooperation' component of cybersecurity has a positive relationship with the development of e-government.

3.3 Conceptual model and hypotheses

The theoretical relationships between the components of cybersecurity and e-government development, as discussed in the previous section, result in five hypotheses.

- **Hypothesis 1 (H1):** The 'legal' component of cybersecurity has a positive relationship with the development of e-government.
- **Hypothesis 2 (H2):** The 'technical' component of cybersecurity has a positive relationship with the development of e-government.
- **Hypothesis 3 (H3):** The 'organisational' component of cybersecurity has a positive relationship with the development of e-government.
- **Hypothesis 4 (H4):** The 'capacity-building' component of cybersecurity has a positive relationship with the development of e-government.
- **Hypothesis 5 (H5):** The 'cooperation' component of cybersecurity has a positive relationship with the development of e-government.

These five hypotheses embody the theoretical relationship between 'cybersecurity' and 'e-government development', as depicted in figure 1.

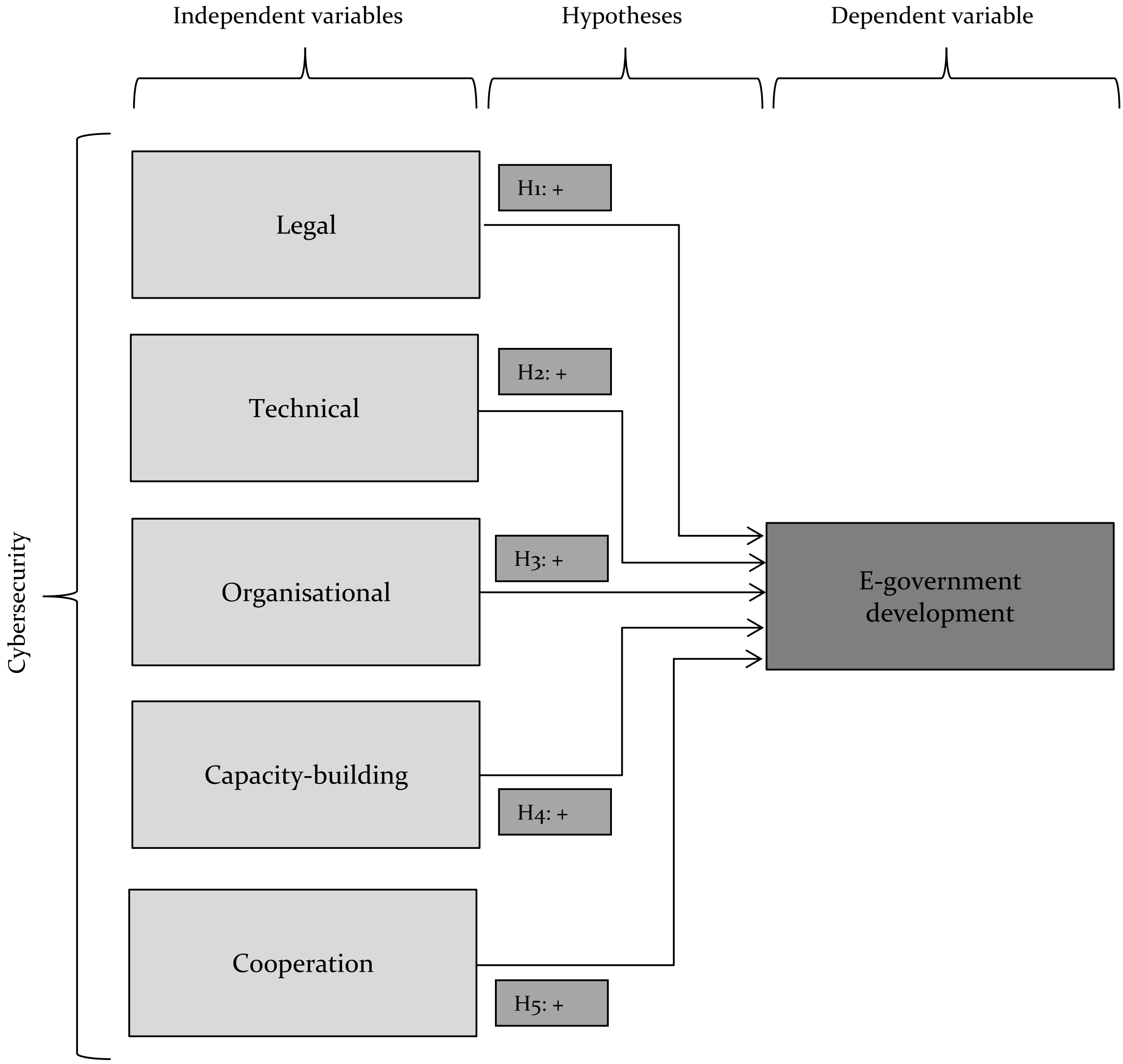

Figure 1 | Conceptual model

To conclude, and answer this study's third sub-question, there is a positive relationship between cybersecurity and e-government development, according to the literature. More specifically, the literature describes positive relationships between all the separate components of cybersecurity (legal, technical, organisational, capacity-building and cooperation) and e-government development, as depicted by the hypotheses and conceptual model of this research.

4 Methodology

This chapter will elaborate on the design of this research, as well as the methods used to conduct the research. This research utilises a panel dataset, composed out of six existing databases: the Global Cybersecurity Index (GCI), the UN E-Government Development Index (EGDI), the Corruption Perception Index (CPI), the Global Innovation Index (GII), the Democracy Index and the World Bank database. Paragraph 4.1 focuses on the collection of data and will therefore present the variables used in this research as well as explain what they are composed of, how they are measured and why they have been chosen. In this section, the descriptive statistics of the variables will also be presented. Subsequently, paragraph 4.2 will elaborate on the method used to measure the relationship between the dependent and independent variables. The validity and reliability of this study will be discussed in paragraph 4.3.

The philosophical underpinning of doing research is *epistemology* ('the science of knowing'), of which an important subfield is *methodology:* 'the science of finding out' (Babbie, 2013). In other words, the methodology describes the procedures and context of the scientific investigation. This way of doing research falls within the philosophical and epistemological discourse of positivism, which assumes that knowledge of a social phenomenon is the result of observation and rational proof/disproof of scientific assertions, and not of subjective understandings or beliefs (Babbie, 2013; Matthews & Ross, 2010). The social reality which is studied is completely independent of the researcher, which makes the researcher objective (Matthews & Ross, 2010). Recently, positivism has been challenged by the idea that researchers cannot be as objective as the positivistic ideal assumes (Babbie, 2013). This new paradigm, called postmodernism, assumes that all experiences and observations are inescapably subjective (Babbie, 2013). The deeper you delve into the roots of the research behind the indexes this study is using, the more one could argue a more postmodernist approach is applicable, as the EGDI and GCI are built upon individual questions (see paragraph 4.1) which inquire a person's subjective observation of reality. Nevertheless, this study assumes the results of these preceding investigations of social phenomena as objective reality and uses these as such in a —therefore predominantly positivist— empirical analysis.

4.1 Data collection

The data collection of research should be determined by the research question and the hypotheses as well as the primary focus points of the research topic (Matthews & Ross, 2010).

This means that the data collection methods depend on the type of data that needs to be collected in order to test the hypotheses and answer the research questions (Matthews & Ross, 2010). This research investigates the relationship between two variables: 1) cybersecurity (independent variable); and 2) e-government development (dependent variable). More specifically, it analyses the relationship of five individual components of 'cybersecurity' with e-government development, namely: legal, technical, organisational, capacity-building, and cooperation. These relationships will be tested by using hypotheses which are based on the theoretical assumptions as outlined in chapter 3. For the data on the variables a panel dataset (explained in 4.1.4) has been created out of existing databases.

4.1.1 Dependent variable

The dependent variable for this study is 'e-government development', as defined by the United Nations as "*the application of ICT in government operations, achieving public ends by digital means*" (United Nations, 2019b). For this variable, this research utilises the existing data from the United Nations E-Government Development Index (EGDI). This database is chosen based on several considerations. Firstly, the assessment of e-government is complex and multidimensional in nature (Siskos, Askounis & Psarras, 2014). This assessment idealistically consists of four important dimensions: 1) infrastructures, 2) investments, 3) e-processes, and 4) users' attitudes (Siskos, Askounis and Psarras, 2014). The UN E-Government Development Index addresses this multidimensional complexity of assessing e-government development. The UN EGDI is a holistic index, based on 2 databases and a survey, which together provide data on three out of the four dimensions mentioned by Siskos, Askounis and Psarras (2014). The EGDI has three sub-indexes: the Telecommunications Infrastructure Index (TII), which assesses infrastructures; the Online Service Index (OCI), which assesses the e-processes; and the Human Capital Index (HCI), which does not directly assess users' attitudes, but demographic (users') characteristics that can be seen as related to users' attitudes. Secondly, e-government can exist at various levels of government, and can therefore also be assessed at these various levels. The UN EGDI examines the development of e-government of its member states on a national level. Since this research requires comparable international data, because it investigates the relationship between cybersecurity and e-government development on a global scale, the UN EGDI lends itself perfectly to provide for this data. Thirdly, the UN EGDI is the most comprehensive and up-to-date database. It encompasses e-government development data of all 193 UN member states (United Nations, 2016) and the UN repeats the research and publication of the EGDI every 2 years, hence never providing data older than 2 years. Lastly, the EGDI is a widely used index in studies that contain (the development of) e-government as a variable (Lee, 2017; Máchová, Volejníková & Lněnička, 2018; Onumo, Cullen & Ullah-Awan, 2017; Verkijika & De Wet, 2016; Wallis & Zhao, 2018). According to Whitmore (2012: p. 68), the EGDI is "the current standard in e-government ranking".

On a biannual basis, the United Nations Department of Economic and Social Affairs (UNDESA), publishes the *United Nations E-Government Survey,* through their Division for Public Administration and Development Management (DPADM). The entire report consists of relevant information to support policy makers in shaping their e-government programmes (United Nations, 2014). Within this report, the EGDI is a composite indicator to measure the willingness and capacity of national governments of all 193 UN member states to use ICTs to deliver public services. The EGDI is not an absolute measurement, as it rates the e-government development of countries relative to each other (United Nations, 2014). In the EGDI, the development of e-government is split in three separate indexes: the Online Service Index (OSI) measuring the scope and quality of online services; the Telecommunication Infrastructure Index (TII) measuring the development status of telecommunication infrastructure; and the Human Capital Index (HCI) measuring the inherent human capital. Each separate dimension is an individual index and the EGDI is a weighted average of three normalised scores on these dimensions:

$$\text{EGDI} = \tfrac{1}{3}\,(\text{OSI}_{\text{normalised}} + \text{TII}_{\text{normalised}} + \text{HCI}_{\text{normalised}})$$

The UN uses a Z-score standardisation procedure to ensure the equal decisive value of each of the sub-indices for the overall score on the EGDI. Subsequently, the composite value of each component index is normalised to fall within the range between 0 and 1, after which the overall EGDI score is decided by the arithmetic average of these scores (United Nations, 2014). Even though the United Nations E-Government Survey has been adjusted over time to reflect new trends in e-government and connecting factors, the methodology of the EGDI, performed by the United Nations has remained consistent to create standardised and comparable results, every edition of the index (United Nations, 2014).

For the data on telecommunication infrastructure (TII), the EGDI uses an arithmetic average of five composite indicators: (estimated) percentage of population that uses the Internet, number of fixed telephone lines per 100 inhabitants, number of mobile (cellular) subscriptions per 100 inhabitants, number of wireless broadband subscriptions per 100 inhabitants and number of fixed broadband subscriptions per 100 inhabitants. The data for these indicators is gathered through data provided by the World Bank and the ITU (United Nations, 2014). For the data on human capital (HCI), the EGDI uses a weighted average of the composite scores on four indicators: adult literacy, gross (school) enrolment ratio, expected years of schooling and mean years of schooling. The data for these indicators is provided by the UN itself (United Nations, 2014). For the data on online service delivery by governments, the EGDI uses data acquired by roughly 100 voluntary researchers (UNVs), consisting of qualified graduate students and volunteers from universities in the field of public administration (United Nations, 2016). The UNVs assess each country's national websites in the native language of the country, including national portals, e-services portals, e-participation portals and websites from specific ministries (United Nations, 2016). All researchers receive rigorous training by e-government and online service delivery experts, to be able to assess the websites from an 'average citizen point of view'[2]. Every country receives a total score for online service provision, which is normalised to the range of 0 to 1. Each country is assessed by at least two researchers, after which the scores are compared with previous years and analysed by UN data team coordinators (United Nations, 2016).

In this study, the separate scores on the sub-indexes of e-government will not be taken into account. Every country's combined score between 0 and 1, indicating the overall e-government development, will be used as data for the dependent variable. This choice has been made because the focus of this study is examining the relationships between the individual components of cybersecurity and e-government development. Looking at the relationship between each individual component of cybersecurity with each individual component of e-government development would drastically increase the amount of hypotheses (to fifteen), which would all require theoretical underpinning. This falls outside of the scope of this study and would be interesting and relevant to investigate in future research (see paragraph 6.3).

4.1.1.1 Descriptive statistics

Before moving to the pooled OLS regression analysis which includes all variables, the characteristics of these individual variables will be outlined using descriptive statistics. In any substantial quantitative work, presenting descriptive statistics is the necessary first step (Mehmetoglu & Jakobsen, 2017). The most important descriptive statistics are central tendency (most commonly presented in the shape of the mean, i.e. arithmetic average) and variability (i.e. standard deviation and range). These descriptive statistics will be presented for the dependent

[2] Relevant features are assessed based on whether they are easy to find and use by an 'average citizen', not whether they in fact exist, but are hidden somewhere on the assessed websites (United Nations, 2014; United Nations, 2016).

and all independent variables after which a histogram of the variable's values is depicted (for the independent variables, see paragraph 4.1.2.1).

The dependent variable, e-government development, is based on an index (EGDI), awarding a score between 0 and 1 for every country (193 in total). The total amount of observations is 386 (193*2). The minimum observed value is 0.0139 (Somalia in 2014) while the maximum observed value is 0.9462 (Republic of Korea in 2014). The mean is 0.482 with a standard deviation of 0.216.

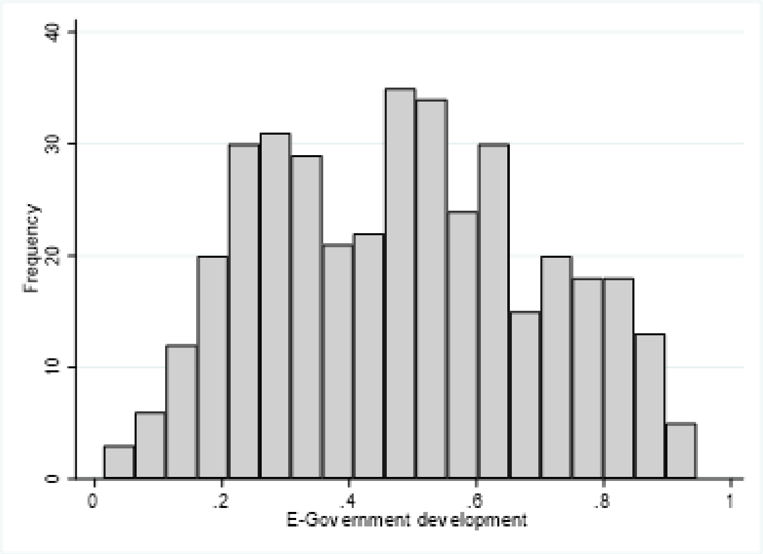

Figure 2 | Histogram DV: E-Government development

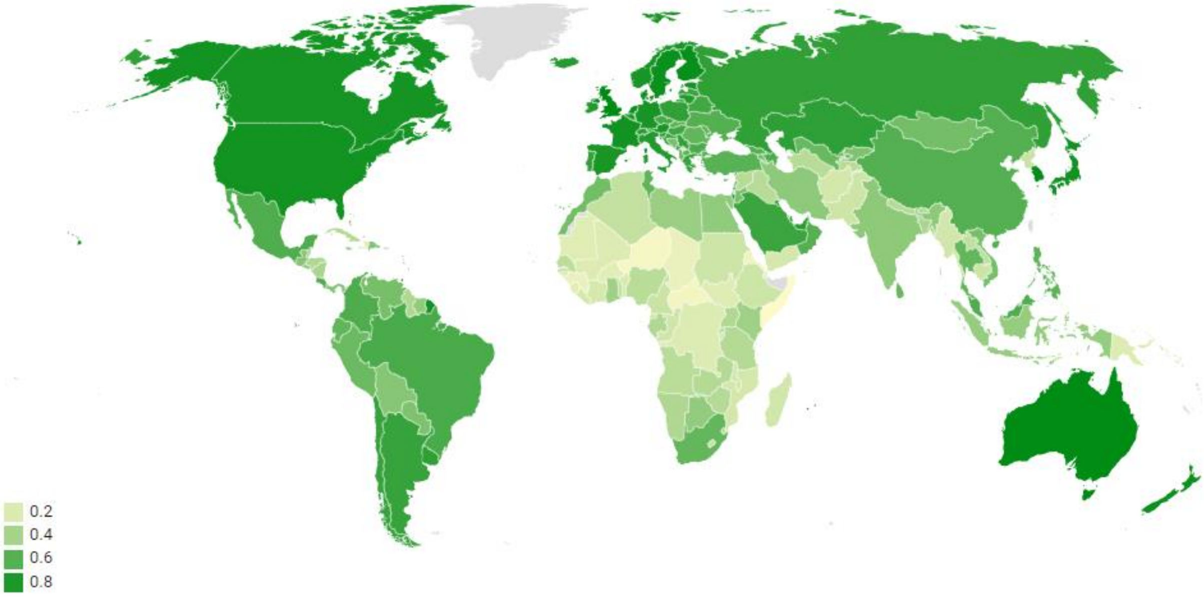

Figure 3 | Country scores on e-government development (source: United Nations, 2014)

4.1.2 Independent variables

The independent variable for this study is 'cybersecurity', as defined by the International Telecommunications Union (ITU) as being the combination of five pillars, that shape the inherent building blocks of a national cybersecurity culture: legal, technical, organisational, capacity-building, and cooperation (ITU, 2018). For this variable, this research utilises another existing dataset, the Global Cybersecurity Index (GCI) by the International Telecommunications Union (ITU). The decision to choose this dataset for the independent variable is because the GCI provides separate data on the sub-domains (pillars), based on a set of indicators, which results in the overall score on cybersecurity of a country. The GCI therefore provides holistic data, which covers all the important components of cybersecurity, which are all expected to have a relationship with the development of e-government (see chapter 3). Thus, the data from this dataset is deliberately chosen, to correspond with the components of a holistic approach to cybersecurity, as described in chapter 2, paragraph 2.2. Additionally, the GCI provides the most up-to-date data, because even though the first edition was only in 2014, the research and publication of the GCI are biannual. Furthermore, the GCI is comprehensive in number of countries observed, because it conducts the research among all 193 member states (ITU, 2017). Moreover, the GCI is used in various studies that contain cybersecurity (commitment) as a variable (Onumo, Cullen & Ullah-Awan, 2017; Verkijika & De Wet, 2016), as well as by the United Nations (2018) to describe the vital elements of a country's resilient digital infrastructure, which is according to the UN, essential for a robust and resilient e-government system (United Nations, 2018).

Since 2014, the ITU conducts an extensive research into the cybersecurity among its member states, which results in the Global Cybersecurity Index (GCI). Following the 2014 iteration, another version was published in 2017, and in 2018 (this last version is still in 'draft phase', see paragraph 4.1.4). The GCI is a composite index of five indices, representing the five aforementioned pillars of cybersecurity. These pillars are in turn composed of 17 (2014) or 25 (2016 and 2018) indicators which represent the content of these pillars and altogether, provide an overview of a country's cybersecurity (ITU, 2017). The indicators are chosen based on 1) the relevance for the five pillars and overall goal of the CGI; 2) data availability and quality; 3) possibility for cross verification through secondary data (ITU, 2017). The indicators of the five pillars of cybersecurity are measured by sending out a questionnaire to the administrations of all ITU member states, regarding the (partial) existence of all indicators in the respective country. After receiving the responses, the results were verified and if necessary sent back to the member states for improvement. After necessary rounds of iteration, the pre-final questionnaire was sent to the member state for approval, and if approved, validated and used for the analysis and ranking (ITU, 2017). In the cases where member states did not respond to the questionnaire, the ITU drafted the responses to the questionnaire by using public data and online research, after which these results were reviewed and validated by the member state.

An important methodological difference between the 2014 GCI on the one hand and the 2017 and 2018 GCIs on the other, is the use of a three-level system in the former and a binary system in the latter (ITU, 2017). Instead of considering 'partial measures' (2014), the later versions of the GCI use a path of binary questions, proceeding 'deeper' into a pillar with each positive answer (similar to the EGDI methodology), resulting in obtaining a higher score on that pillar (ITU, 2017). This difference in methodology means that for the scores, the 2014 GCI uses a simple average while the 2017 and 2018 version use a weighted factor. Nevertheless, both methods use the same pillars and (largely) the same indicators to determine the scores, which in both methods is presented as a number in the range of 0 to 1 (for the overall score and for each pillar separately). The next section contains an elaboration on the meaning and indicators of each pillar.

Legal

Legislation provides the framework for behavioural standards regarding cyber activities and provide the legitimisation for prosecution of cybercriminal behaviour. The legal component of cybersecurity is measured through the following indicators (ITU, 2014; ITU, 2017):

a. Cybercriminal legislation: laws on the unauthorised access, interference or interception of computers, systems or data;
b. Regulation and compliance: these concern laws and regulations focusing on data protection, breach notification and certification/standardization requirements;
c. Cybersecurity training[3].

Technical

Adequate technical measures are the first line of defence against cyber-threats and are measured by existence and number of technical institutions and frameworks focused on cybersecurity, comprised in the following indicators (ITU, 2014; ITU, 2017):

[3] These indicators were added for the 2017 and 2018 GCI and were therefore not part of the 2014 GCI.

a. National Computer Incident Response Teams (CIRT): these teams provide the capabilities to identify, defend, respond and manage cyber threats and enhance national cybersecurity;
b. Government CIRTs[3];
c. Sectoral CIRTs[3];
d. Standards for organisations: these include the existence of government-approved framework(s) for the implementation of cybersecurity standards within the public sector and critical infrastructure (also when privately operated);
e. Standards and certification for professionals: these include the existence of government-approved framework(s) for the certification and accreditation national (government) agencies and public sector professionals by internationally recognised cybersecurity standards;
f. Child online protection[3].

Organisational

Organisational and procedural measures, such as a broad strategy with a plan of implementation, is needed for the implementation for national cybersecurity initiatives (ITU, 2014). These are being measured by the following indicators (ITU, 2014; ITU, 2017):

a. A national policy and roadmap: these include a national cybersecurity or information infrastructure protection strategy, and a roadmap for governance identifying the stakeholders within this strategy;
b. Responsible agency: these include committees, working groups, advisory councils or cross-disciplinary centres responsible for implementing the national cybersecurity policy/strategy;
c. National benchmarking/cybersecurity metrics: this includes the existence of officially recognised national or sector-specific benchmarking and cybersecurity metrics used for cybersecurity development.

Capacity-building

This pillar is intrinsic to the previous three and focuses on the socio-economic and political implications of the relatively new field of cybersecurity, which in turn help develop better legislation, policies and strategies and organisations. Capacity-building consists of the following indicators (ITU, 2014; ITU 2016):

a. Standardisation development/bodies: increased standardisation and use of commonly recognised standards in key areas;
b. Manpower development/public awareness: these include widespread publicity and awareness campaigns concerning safe cyber-behaviour;
c. Professional- and agency certification: these are public sector professionals and agencies certified under internationally recognised certifications;
d. Good practices[3];
e. R&D programmes[3];
f. Professional training courses[3];
g. National education programmes and academic curricula[3];
h. Incentive mechanisms[3];
i. Home-grown cybersecurity industry[3].

Cooperation

This pillar looks at cybersecurity initiatives with a multi-stakeholder approach, and includes the following indicators (ITU, 2014; ITU 2016):

a. Intra-state cooperation: officially recognised national or sector-specific partnerships for sharing cybersecurity assets with other countries;
b. Intra-agency cooperation: officially recognised national or sector-specific partnerships for sharing cybersecurity assets within the public sector;
c. Public-private partnerships: joint cybersecurity ventures between the public and private sector;
d. International cooperation: participation in international cybersecurity platforms and forums;
e. Multilateral agreements[3].

In the GCI (2014 and 2016), every country has a score in the range between 0 and 1 on all five pillars separately, which will be used in this study as the data for the independent variables. All countries also have an overall 'cybersecurity' score, which will not be used in this study.

4.1.2.1 Descriptive statistics

The independent variables in the model — legal, technical, organisational, capacity-building and cooperation — are all based on sub-indexes of the Global Cybersecurity Index (GCI), which each award every country with a score between 0 and 1. Since 0 and 1 are regularly awarded scores for these sub-indexes, the minimum and maximum observed values for the independent variables are most often respectively 0 and 1, with many observations having that value.

The independent variable ‘legal’ has a total amount of 386 observations, with a minimum observed value of 0 (multiple observations) and a maximum observed value of 1 (multiple observations). The mean is 0.470 with a standard deviation of 0.330.

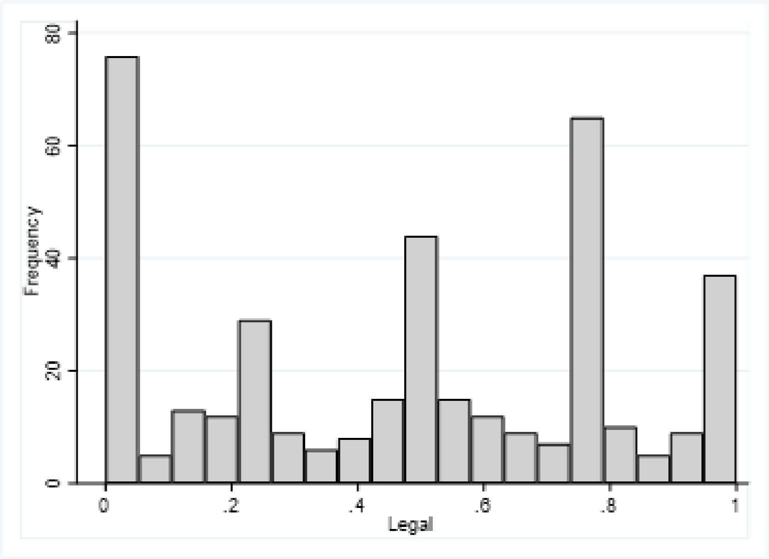

Figure 4 | Histogram IV: Legal

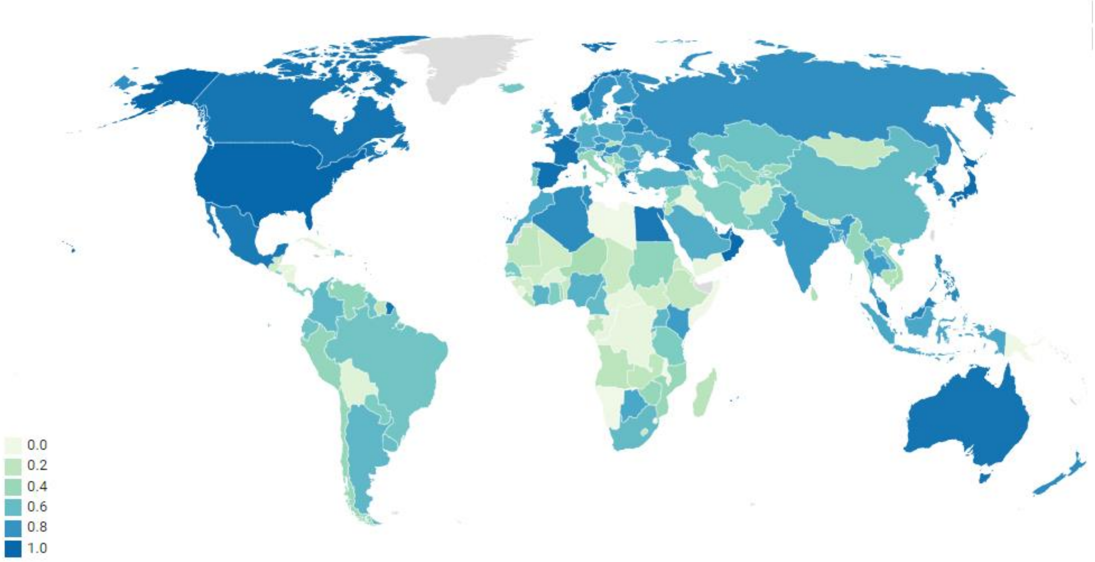

Figure 5 | Country scores on 'legal' (source: ITU, 2016)

The independent variable ‘technical’ has a total amount of 386 observations, with a minimum observed value of 0 (multiple observations) and a maximum observed value of 1 (multiple observations). The mean is 0.320 with a standard deviation of 0.310.

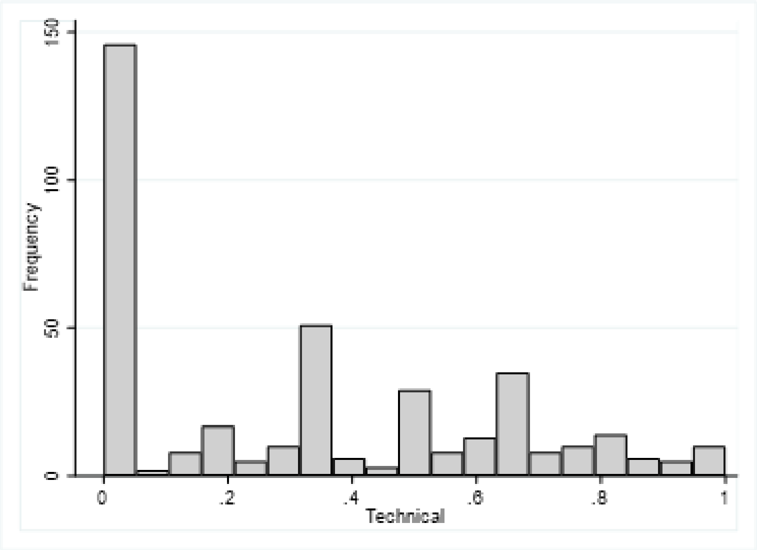

Figure 6 | Histogram IV: Technical

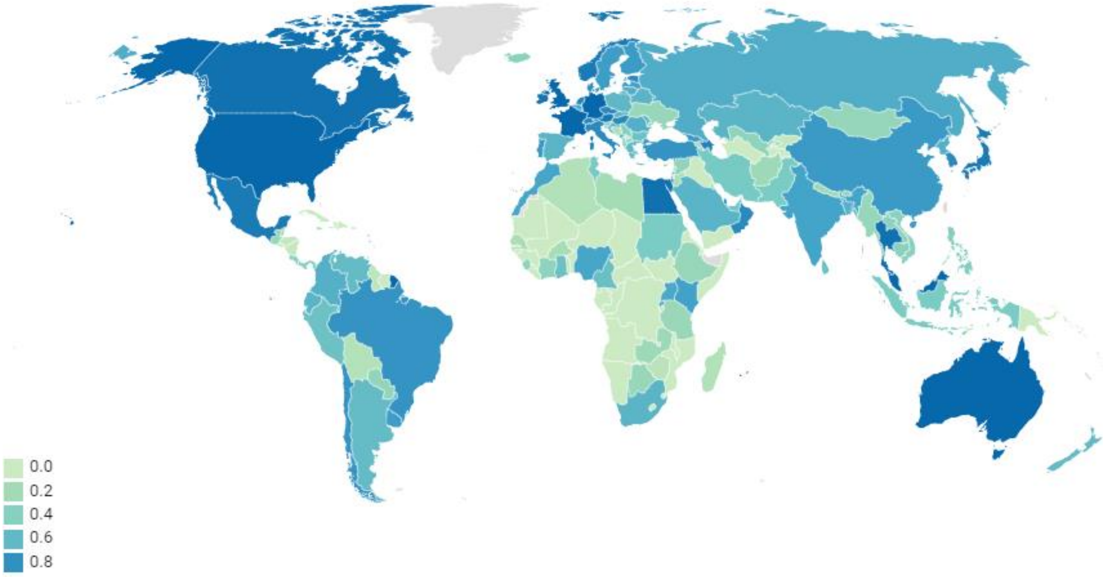

Figure 7 | Country scores on 'technical' (source: ITU, 2016)

The independent variable ‘organisational’ has a total amount of 386 observations, with a minimum observed value of 0 (multiple observations) and a maximum observed value of 1 (multiple observations). The mean is 0.289 with a standard deviation of 0.270.

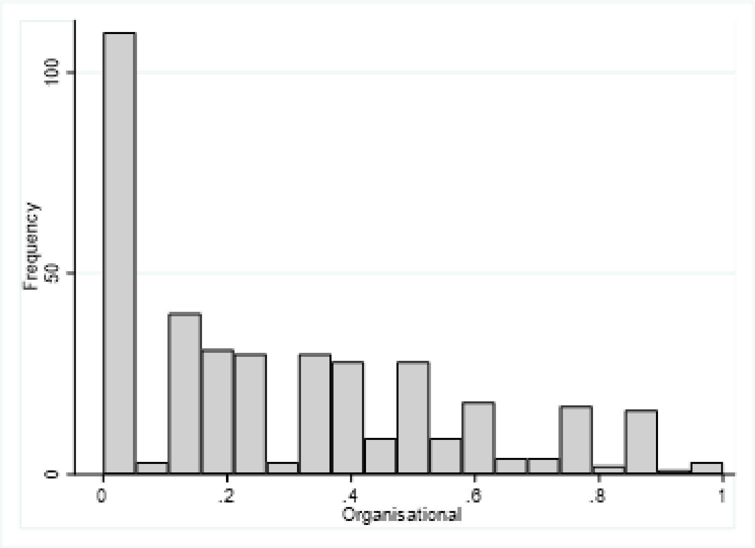

Figure 8 | Histogram IV: Organisational

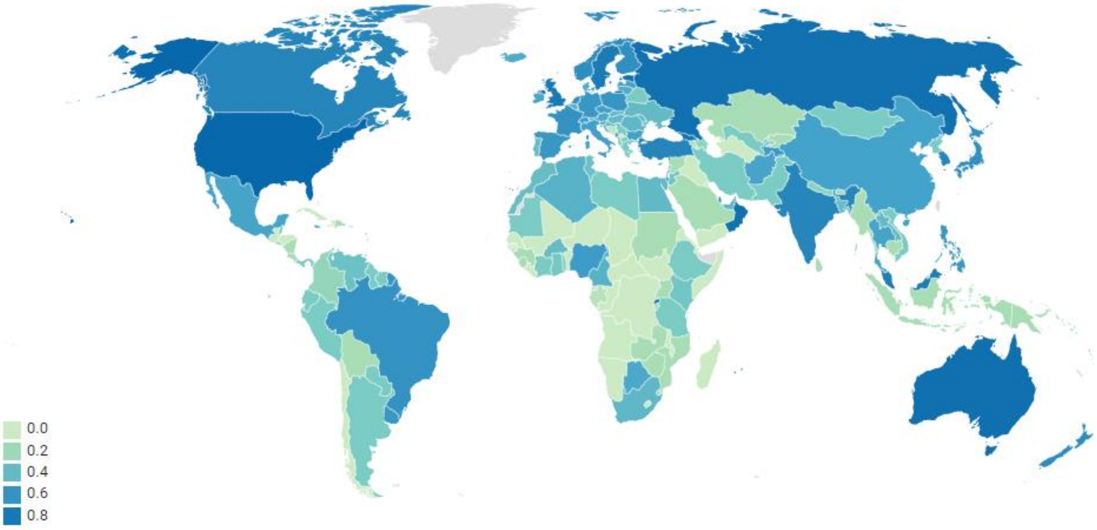

Figure 9 | Country scores on 'organisational' (source: ITU, 2016)

The independent variable 'capacity-building' has a total amount of 386 observations, with a minimum observed value of 0 (multiple observations) and a maximum observed value of 1 (multiple observations). The mean is 0.284 with a standard deviation of 0.294.

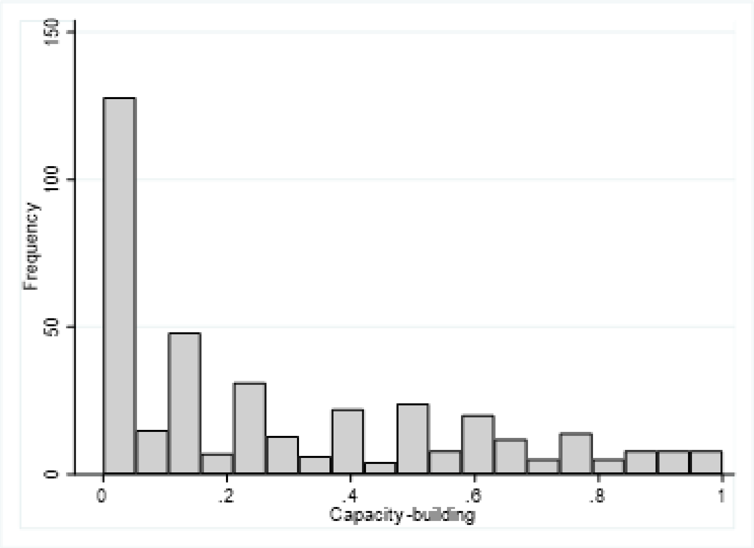

Figure 10 | Histogram IV: Capacity-building

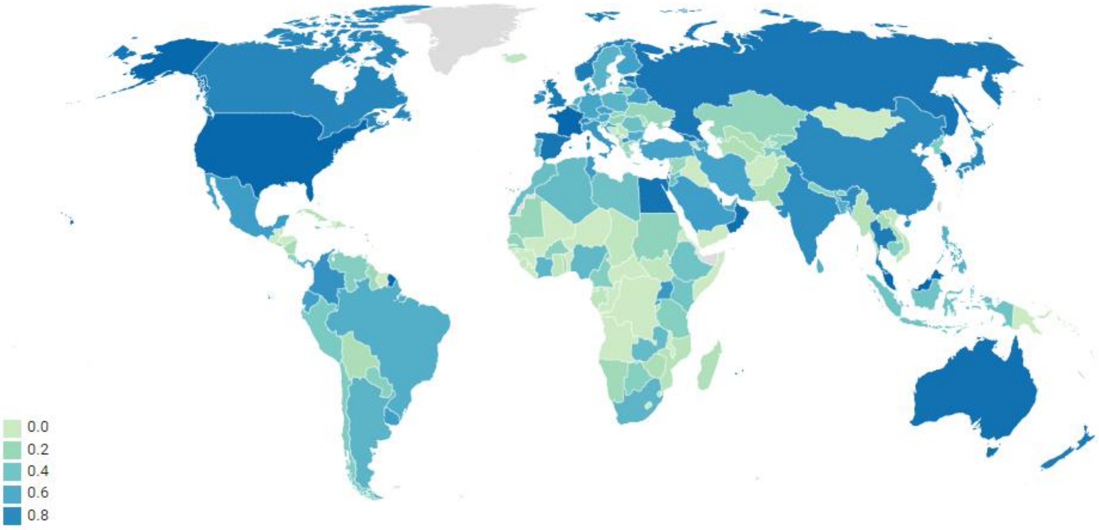

Figure 11 | Country scores on 'capacity-building' (source: ITU, 2016)

The independent variable ‘cooperation’ has a total amount of 386 observations with a minimum observed value of 0 (multiple observations) and a maximum observed value of 0.871 (Finland in 2016). The mean is 0.291 with a standard deviation of 0.211.

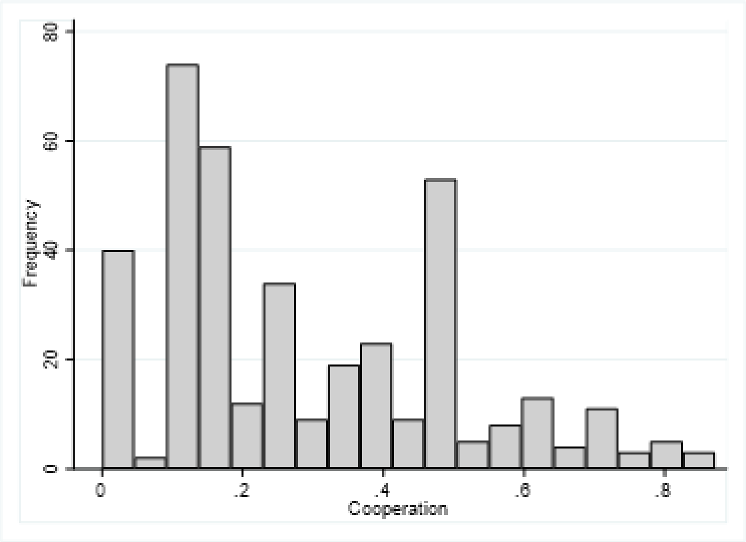

Figure 12 | Histogram IV: Cooperation

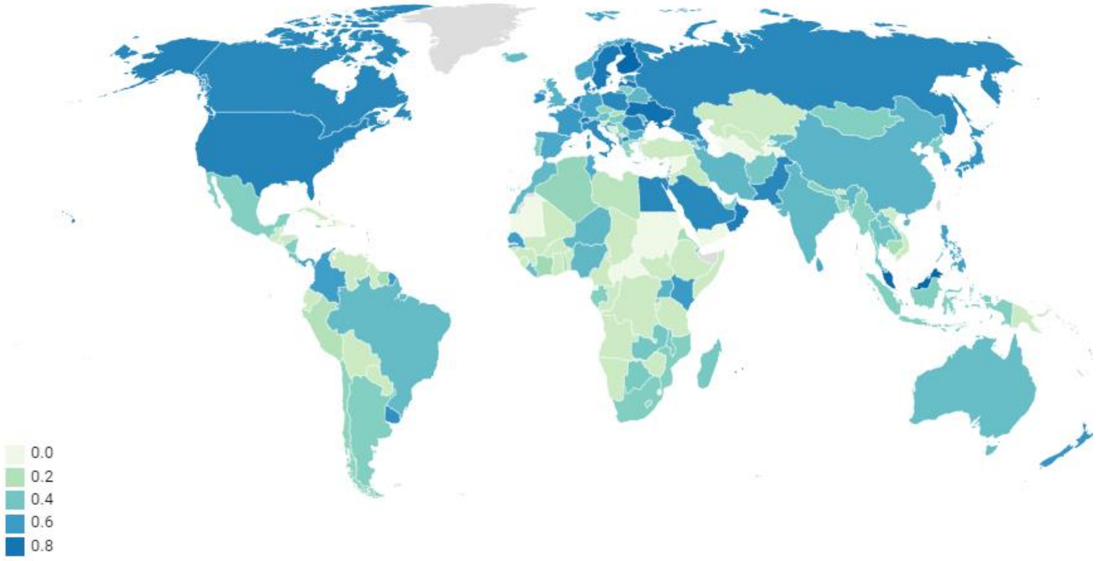

Figure 13 | Country scores on 'cooperation' (source: ITU, 2016)

4.1.3 Control variables

Performing a statistical analysis of the relationship between two or more variables by using existing data inherently includes the risk of spurious effects, i.e. effects caused by non-focal variables (Bernerth & Aguinis, 2016). Alternative for controlling for these effects in a time- and resource-costly (quasi) experimental design, using statistical control variables is a practical and feasible way of controlling for these spurious effects. By including confounding variables, the usage of statistical control variables mathematically removes the effects of non-focal variables (Bernerth & Aguinis, 2016).

To select the control variables, a literature review is conducted into studies that take on a 'government-centric' approach concerning e-government and therefore not assessing factors that influence adoption of e-government by citizens (end users). The two most relevant studies are the ones by Kabanov and Sungurov (2016) and Verkijika and De Wet (2016). Unfortunately, the first study is published in an article which is neither an open access source, nor accessible through journal subscriptions of the Erasmus University Rotterdam. This also applies for the latter, although the article by Verkijika and De Wet (2016) was received via e-mail after contacting one of the authors. Verkijika and De Wet (2016) emphasize an important confounding variable for e-government development, which the United Nations (2018) themselves also mention in their reports on e-government development: national income. The national income (in US$) of a country reflects its economic progress, and previous reports by the UN found a relationship between national income and e-government development (Hafeez & Sher, 2006). This indicator is measured by data on national income by the World Bank, expressed in GNI (gross national income) in US dollars (US$). The descriptive statistics in this study show that 'national income' has a total amount of observations of 370, with a minimum observed value of $49,698,846 (Tuvalu in 2014) and a maximum observed value of $\$1.905 \cdot 10^{13}$ (United States of America in 2016). The mean is $\$4.13 \cdot 10^{11}$ with a standard deviation of $\$1.68 \cdot 10^{12}$. The descriptive statistics of this control variable show a distribution that is positively skewed, i.e. the distribution is asymmetric. Usually, this is solved by log-transforming the variable, which replaces its values with its decadic logarithm. However, there are three reasons why 'national income' is not log-transformed in this study, namely 1) 'national income' is a control variable, not a focal variable and serves to control for spurious effects within the model, 2) direct interpretation of the variable becomes more difficult after transformation (Mehmetoglu & Jakobsen, 2017), and 3) variables being normally distributed is not one of the assumptions necessary to be met for a regression analysis (see paragraph 4.2.3).

Another confounding variable used in the study by Verkijika and de Wet (2016) is corruption. Corruption can be seen as an important factor in the development and maturity of e-government projects, especially visible in developing regions where there is a high degree of failure of e-government projects (Aladwani, 2016; Singh, Das & Joseph, 2007; Verkijika & De Wet, 2016). This indicator is measured by the Corruption Perception Index by Transparency International. Each country receives a score in the range between 0 (very corrupt) and 100 (very clean) (Transparency International, 2018). The descriptive statistics in this study show that 'corruption' has a total amount of 341 observations with a minimum observed value of 8 (Democratic People's Republic of Korea in 2014 and Somalia in 2014) and a maximum observed value of 92 (Denmark in 2014). The mean is 42.848 with a standard deviation of 19.556.

A third variable which is perceived to have an influence on e-government development is innovation. Innovation, commonly referred to as the transformation of an invention to create ways of adding value, is important for e-government development as it is necessary for the initiation and improvement of e-government initiatives (Kim, Pan & Pan, 2007; Verkijika & De Wet, 2016). Countries with high levels of innovation are perceived to be positive towards adopting new approaches and thus have a higher likelihood to initiate and develop e-government systems (Anthopoulos, Reddick, Giannakidou & Mavridis, 2015). This variable is measured by the Global Innovation Index (GII), which is a joint publication by the World Intellectual Property Organisation (WIPO), Cornell University and INSEAD. Each country receives a score in the range between 0 and 100 (Dutta, Lanvin, & Wunsch-Vincent, 2016). The descriptive statistics in this study show that 'innovation' has a total amount of 269 observations with a minimum observed value of 12.66 (Sudan in 2014) and a maximum observed value of 66.28 (Switzerland in 2016). The mean is 36.679 with a standard deviation of 11.559.

Next to national income, corruption and innovation, the study by Verkijika and De Wet (2016) examined three other variables, of which one is examined in this study as independent variable (cybersecurity) and two are perceived as explanatory variables for e-government *adoption* by individual citizens (gender equality and age differences), not for e-government *development* by national governments. These variables are therefore not included as control variables.

A fourth relevant factor for the explanation of variance of e-government development, is quality of government. A good indicator for quality of government is 'government effectiveness', which is one of the six Worldwide Governance Indicators used by the World Bank (Kaufmann, Kraay & Mastruzzi, 2003). Government effectiveness refers to the quality of public service provision, the quality of the bureaucracy, the competence of civil servants, the independence of the civil service from political pressures and the credibility of the government's commitment to policies (Kaufmann, Kraay & Mastruzzi, 2003). Previous research by Kim (2007) and Wallis and Zhao (2018) shows that government effectiveness is a very important determinant for e-government development and performance. Government effectiveness was added to the model as control variable. However, the regression assumption tests (see paragraph 4.2.3) showed that this variable has a very high degree of multicollinearity. This means that various variables steal explanatory power from each other, i.e. that multiple variables measure the same phenomenon (Mehmetoglu & Jakobsen, 2017). The solution for multicollinearity is to remove the variable from the model. Therefore, government effectiveness is not included into the model. Instead, another variable related to the quality of government is included, namely 'state of democracy'. The relationship between (the state of) a democratic regime and the e-government has previously been assumed and tested by Kabanov and Sungurov (2016), who concluded that the state of democracy is an important predictor for the maturity of e-government. The level of democracy is measured by Democracy Index, which is a yearly global ranking of the state of democracy in 165 countries, conducted by the Economist Intelligence Unit. The Democracy Index is based on five categories: electoral process and pluralism; civil liberties; the functioning of government; political participation; and political culture. Especially the category 'functioning of government' resembles the 'government effectiveness' variable. Each country receives a score between 0 and 10 (The Economist Intelligence Unit, 2014). The descriptive statistics in this study show that 'state of democracy' has a total amount of 328 observations with a minimum value of 1.08 (Democratic People's Republic of Korea in 2014 and 2016) and a maximum value of 9.93 (Norway in 2014 and 2016). The mean is 5.520 with a standard deviation of 2.194.

The operationalisation of all variables, with corresponding indicators, definitions, organisations and databases are presented in table 1.

Table 3 | Operationalisation of variables

Type	Variable		Indicators	Definition of indicator	Database	Organisation
DV	E-government development		National e-government development score	National, relative to each other, e-government development score based on composite indices .[4]	EGDI	UN
IV	Cybersecurity	Legal	National ‘legal’ score	The existence and number of legal institutions and frameworks dealing with cybercrime.[5]	GCI	ITU
		Technical	National ‘technical’ score	The existence and number of technical institutions and frameworks dealing with cybersecurity endorsed or created by the nation state.[5]	GCI	ITU
		Organisational	National ‘organisational’ score	The existence and number of institutions and strategies organizing cybersecurity development at the national level.[5]	GCI	ITU
		Capacity-building	National ‘capacity-building’ score	The existence and number of research and development, education and training programs, and certified professionals and public sector agencies.[5]	GCI	ITU
		Cooperation	National ‘cooperation’ score	The existence and number of partnerships, cooperative frameworks and information sharing networks.[5]	GCI	ITU
CV	National income		GNI (Gross National Income) in US$	The sum of value added by all resident producers plus any product taxes not included in the valuation of output, plus net receipts of primary income from abroad.[6]	World Bank database	World Bank
	Corruption		National corruption perception score	Perceived levels of national public sector corruption on a global scale .[7]	Corruption Perception Index (CPI)	Transparency International

[4] United Nations, 2019b

[5] ITU, 2014

[6] World Bank, 2019

[7] Transparency International, 2018

	Innovation	National innovation score	National innovation score based on composite sub-indices.[8]	Global Innovation Index (GII)	WIPO/Cornell / INSEAD
	State of democracy	National democracy score	National score on the state of democracy, based on five categories.[9]	Democracy Index	The Economist Intelligence Unit

Following the descriptive statistics of each individual variable, a Pearson correlation test was conducted to find correlation between variables in the model.

Table 4 | Correlation matrix

		A	B	C	D	E	F	G	H	I	J
A	E-Gov. Dev.[10]	1.00									
B	Legal	0.666	1.00								
C	Technical	0.662	0.649	1.00							
D	Organisational	0.597	0.627	0.772	1.00						
E	Capacity-B[11]	0.631	0.631	0.852	0.769	1.00					
F	Cooperation	0.573	0.559	0.700	0.661	0.733	1.00				
G	Nat. income[12]	0.287	0.262	0.309	0.302	0.365	0.253	1.00			
H	Corruption	0.758	0.495	0.505	0.509	0.507	0.488	0.218	1.00		
I	Innovation	0.840	0.505	0.582	0.563	0.535	0.516	0.347	0.846	1.00	
J	State of Dem.[13]	0.651	0.428	0.476	0.482	0.438	0.456	0.154	0.736	0.674	1.00

The correlation matrix shows that except for 'national income', there is a moderately to high correlation between all the independent variables and control variables on the one hand and the dependent variable on the other. The high correlation values in column A (between e-government development on the one hand and 'legal', 'technical', 'capacity-building', 'corruption', 'innovation' and 'state of democracy' on the other) means that the explanatory value for 'e-government development' of these variables is high, while for 'organisational' and 'cooperation' this is less the case and for 'national income' to a very little extent. Whether the relationships between these variables and 'e-government development' are also significant, will become clear after conducting a pooled OLS regression analysis, of which the results are presented in chapter 5.

[8] Dutta, Lanvin, & Wunsch-Vincent, 2016
[9] The Economist Intelligence Unit, 2014
[10] E-Government development
[11] Capacity-building
[12] National income
[13] State of democracy

4.1.4 Case selection and organising the data

From these databases, a panel dataset was created. A panel data study is a longitudinal study in which data is collected from the same set of cases (panel) (Babbie, 2013). Simply put, a panel dataset consists of a specified set of units that have observations on different points in time (Kennedy, 2008). Studies making use of panel data analysis have been growing in prevalence, largely catalysed by the growing number of existing databases (Hsiao, 2007). Panel data studies allow for integrated cross-sectional and time series analyses, because data is used from different individual cases, over at least two points in time. This creates opportunities for more complex statistical analyses and provides truer estimates of the effects of explanatory variables (Hsiao, 2007; Mehmetoglu & Jakobsen, 2017). Furthermore, with repeated observations on the same unit, panel dataset are able to control for unobserved explanatory variables (controlling for individual heterogeneity) (Mehmetoglu & Jakobsen, 2017). Moreover, according to Baltagi (2001: p. 6), "panel data give more informative data, more variability, less collinearity among the variables, more degree of freedom and more efficiency".

The initial panel dataset for this study consists of the data of 193 countries, for the aforementioned nine variables, of the years 2014 and 2016. That makes this panel data set a 'short panel', with many entities (large *n*), which is wide in width (cross-sectional) and short in length (time-series). Contrary to that, there are 'long panels', with a smaller *n* and (narrow in width) but many time periods (*i*) (Park, 2011). This choice is based on the availability of data provided by the databases. The EGDI is published every 2 years, so the data of the 2014 and 2016 edition is used for this research. The GCI was first published in 2014, and subsequently in 2017 and in 2018. Even though the second edition of the GCI was published in 2017, the entire research for this edition was conducted from January to September 2016 (ITU, 2017). This has led to the decision to consider this edition as sufficient to provide the data for the cybersecurity variable for the first point in time (2016). To be able to test the relationship between all individual components of cybersecurity with e-government development, scores per country on the five separate pillars within the GCI are necessary. The 2014 edition of the GCI provides this level of detailed data, but the 2017 edition unfortunately not. This edition only provides this for the top-10 ranked countries. For the latest edition, the GCI from 2018, this is also the case. Because of this, the ITU was contacted via e-mail, with the inquiry whether a complete dataset could be provided for the GCI editions of 2017 and 2018. For the 2017 edition this was possible, and the dataset was provided. For the 2018 edition, this was not possible, because this edition was still in 'draft phase', hence no detailed data per country was available. This limited the time-series possibilities of this research, because despite the availability of detailed data on e-government development from 2018, for cybersecurity, detailed data is only available for the years 2014 and 2016.

Next to limited availability of temporal data, there is also a slight variety of availability of data between the EGDI and the GCI concerning the number of cases. For both the 2014 and the 2016 EGDI, data is provided for all UN member states, i.e. 193 cases. The 2014 GCI provides the data for 195 member states, while the 2017 edition of the GCI included 194 member states. The higher number of cases in the GCI can be explained by the inclusion of Hong Kong and the State of Palestine in 2014, and the inclusion of the State of Palestine in 2017. Since Hong Kong is excluded from the GCI since 2017 and the EGDI neither provides data for Hong Kong, nor for the State of Palestine, these cases will be excluded from the panel in this research.

After deciding on which database is used for the data on every variable, as well as the years and countries of exclusion, the data needs to be organised. For a proper organising and structuring of the data, Windows Excel and Stata software were used. First, the data of all variables was processed and structured into Excel, after which it was confirmed into Stata to be able to perform various descriptive analyses and a pooled OLS regression analysis, as of which the findings are presented in chapter 5. The dataset that has been created was organised along three different dimensions: the first dimension is *units* expressed as $i = 1, \dots, n$; the second is *measurements* (panel waves/points in time) expressed as $t = 1, \dots, T$; and the third is *variables* expressed as $v = 1, \dots, V$. Herein, the *units (i)* are the objects of analysis, which are the 193 countries that are included in this study: $i = 193$; the *measurements* are the two years (2014 and 2016) included in the study: $t = 2$; the *variables* are all variables combined: $v = 9$. The higher the amount of observations, the higher the risk for (systematic) dropout within the panel dataset (Mehmetoglu & Jakobsen, 2017). This is also the case in this study, as the control variables have missing values for a number of countries. For the control variables national income, corruption, state of democracy and innovation there are respectively 16, 45, 58 and 117 missing values, which means that these observations have been deleted from the dataset, resulting in $n = 269$ instead of $n = 386$. The decrease in n lowers generalisability. Nevertheless, a remaining n of 269, plus the fact that the countries have an observation for multiple points in time, makes trustworthy correlational analysis possible (Mehmetoglu & Jakobsen, 2017).

4.2 Statistical analysis

4.2.1 Panel data analysis

When all data is structured along the aforementioned dimensions (*i, t,* and *v*), it is possible to conduct panel data analyses. As mentioned, panel data analyses combine (at least) two dimensions, the cross-sectional dimension and the time-series dimension (Hsiao, 2007; Kennedy, 2008). This is especially useful in the social sciences, as many of them usually combine time-series and cross-sections of units in data (Greene, 2012).

The data for this study is extracted from databases which are being published on a regular basis at different points in time, which makes it eligible for a panel data analysis. For this study, the observations of the units (193 countries) for the various variables are examined in two points in time: the years 2014 and 2016. Datasets like these one allow for more complex statistical analyses because the multidimensional data over 2 points in time ensure individual heterogeneity (Baltagi, 2008), control for the impact of omitted variables (Hsiao, 2007) and give less collinearity between variables (Gil-Garcia & Puron-Cid, 2015). Panel data analyses also have disadvantages, mainly connected to generating the data. An often used instrument for generating panel set data is the use of survey questionnaires, which has risks related to inadequate sampling of target populations, faulty question design and non-/late response (Hsiao, 1986). In this study, these risks are mitigated by selecting data from existing databases, creating a custom panel.

4.2.2 Pooled OLS regression analysis

With a prepared panel dataset, one can perform a simple linear regression analysis, named pooled Ordinary Least Squares (OLS) regression (Gil-Garcia & Puron-Cid, 2015). Given the assumption that each unit in the panel data has multiple observations, which are nested and therefore not independent of each other, the pooled OLS regression analysis is able to estimate coefficients in this panel data (Mehmetoglu & Jakobsen, 2017). Conducting this analysis provides information on the existence and strength of correlation between the components of cybersecurity (independent variables) and the development of e-government (dependent variable). When conducting an OLS regression analysis, the assumption is a fully pooled model:

$$Y_{it} = \beta_0 + \beta x_{1it} + \varepsilon_{it}$$

A fully pooled model includes units that all obey the same specification with the same parameter values (Mehmetoglu & Jakoben, 2017). The equation for the pooled OLS regression analysis conducted in this study follows from including all the variables into the fully pooled model:

$$Y_{it} = \beta_0 + x_{1it}\,\beta_1 + x_{2it}\,\beta_2 + x_{3it}\beta_3 + x_{4it}\,\beta_4 + x_{5it}\,\beta_5 + Z_{it} + \varepsilon_{it}$$

In this equation, Y_{it} is the dependent variable, e-government development, in country *i* and in year *t*, while the subsequent x_{1it} until x_{5it} are representing the independent variables: legal, technical, organisational, capacity-building and cooperation, for country *i* and year *t.* Z_{it} represents the control variables, national income, corruption and innovation and state of democracy, in country *i* and year *t,* whereas ε_{it} stands for the margin of error. The β_1 to β_5 indicate the regression coefficient (slope) for that specific independent variable (Torres-Reyna, 2007). Conducting a pooled OLS regression analysis provides insight in the values of β_1 to β_5, which determines the slope of the regression. The regression coefficient (or slope) of a regression shows the amount of (average) change in Y (dependent variable) for every unit increase in X (independent variable), hence shedding light on the relationship between the independent variables and the dependent variable (Mehmetoglu & Jakobsen, 2017).

4.2.3 Regression assumptions

When conducting any form of regression analysis, there are certain assumptions that must be met. If the model of the analysis does not adhere to these assumptions, it is not possible to trust the estimates of the model (Mehmetoglu & Jakobsen, 2017). Before conducting the pooled OLS regression analysis, the relevant regression assumptions were tested (see table 4).

Table 5 | Regression assumptions

Test	Desired outcome	Outcome
Wooldridge test	> 0.01	N/A
Breusch-Pagan hettest	> 0.05	Chi2 (1): 11.137 p-value: 0.001
Variance inflator factor (VIF)	< 5.00	Innovation: 4.42 Corruption: 4.14 Capacity-building: 3.47 Technical: 3.15 Organisational: 2.67 Cooperation: 2.23 State of democracy: 2.10 Legal: 1.75 National income: 1.23
Shapiro-Wilk normality test	> 0.01	z: 0.605 p-value: 0.273
Cook's distance	< 1.00	No distance is above the cut-off

The first regression assumption is that there is no autocorrelation. For panel data, autocorrelation means that observations of the same units are not completely independent from each other, but correlated (Drukker, 2003). One year's value might be of influence for the next year's, which means the observations would be connected. This is more likely to occur in time-series or panel data, since observations of the same unit in different time periods can be connected to each other. To test this regression assumption in panel data, one can use the Wooldridge test, which was initially attempted in this study as well. However, to conduct the Wooldridge test for autocorrelation, the panel dataset needs to have a minimum of three time periods (Mehmetoglu & Jakobsen, 2017). This is not the case in this study, which only has data for two time periods: 2014 and 2016. For this reason, the Wooldridge test could not be conducted.

Autocorrelation can lead to correlation between the independent variables and the error term, which may result in heteroscedasticity (Mehmetoglu & Jakobsen, 2017). Heteroscedasticity occurs when the regression model predicts some values of the dependent variable more precisely than others. In other words, there is homoscedasticity when the variance of the outcome variable (Y) is stable at all levels of the predictive variable (X), so that errors are both independent of each other and normally distributed (Mehmetoglu & Jakobsen, 2017). Testing for heteroscedasticity was done by conducting the Breusch-Pagan hettest. In the case of a significant result (< 0.05) there is heteroscedasticity, which is the case in this study (p-value is 0.001), thus there is heteroscedasticity in the model. To control for this, robust standard errors are used, which do not change coefficient estimated, but do change the standard errors which leads to reasonably accurate p-values (Mehmetoglu & Jakobsen, 2017).

The Variance Inflator Factor (VIF) test is the third test that was conducted, which is a test for multicollinearity. Multicollinearity occurs when explanatory variables (X) are not completely independent of each other (Farrar & Glauber, 1967). This can result in difficulties in assessing the relative importance of the different individual independent variables (Mehmetoglu & Jakobsen, 2017). The solution for problems with multicollinearity is either the exclusion of an explanatory variable, or the merging of two explanatory variables which (largely) measure the same phenomenon (Mehmetoglu & Jakobsen, 2017). Multicollinearity tested through the VIF test should result in a score no higher than 5 for each variable. The results show that this is not the case for any variable in this study, which means there is no multicollinearity between variables.

Subsequently, the Shapiro-Wilk normality test was conducted to test whether the data sample is taken from a normally distributed population. A normally distributed population —and thus normally distributed errors in the regression model — are necessary for valid statistical generalisation (Mehmetoglu & Jakobsen, 2017). Would the Shapiro-Wilk test result in a significant outcome of < 0.01, then the data sample is not from a normally distributed population. This is not the case in this study, since the outcome of the Shapiro-Wilk test is higher than 0.01. Ergo, the population in the sample of the panel dataset is normally distributed.

The last test that was conducted is the Cook's distance, which estimates the influence of single outlier observations on the model as a whole. Outlier observations are observations with an unusual value, which can affect the calculation of the regression coefficients (slope), the standard errors and the R-squared (Mehmetoglu & Jakobsen, 2017). Conducting the Cook's distance test provides the knowledge that there is no distance above the cut-off, i.e. that model does not contain influential outliers.

5 Results

In this chapter, the results of the empirical analysis in this research will be presented. Herewith, sub-questions 3 (*what is the state of cybersecurity in a global context?)* and 4 (*what is the level of e-government development in a global context?)* of this study will be answered. Paragraph 5.1 will present and describe the results of the pooled OLS regression analysis.

5.1 Pooled OLS regression analysis

After having established correlation between multiple variables in the model, the pooled OLS regression analysis will provide insight about whether these correlations are then also significant. The null hypotheses in this study is the non-existence of a relationship between any of the explanatory variables (independent and control variables) with the outcome variable (dependent variable). In table 3, all results of the pooled OLS regression analysis are presented, including the *p*-value. The closer the *p*-value of an independent variable is to zero, the more certain it can be stated that the hypothesis for that variable proposed in this study is more likely than the null hypothesis (significance) (Mehmetoglu & Jakobsen, 2017).

Null hypothesis (H_0) F-test: *There is no relationship between any of the explanatory variables and the outcome variable.*

The information regarding this null hypothesis is provided by the F-test. The F-test has a null hypothesis that the R-squared value is zero, meaning that the explanatory factors in the model explain the outcome variable for 0 per cent. Alternatively, an R-squared score higher than 0 indicates for how many per cent (after multiplied by 100) the explanatory variables in the model explain for the outcome variable (Park, 2011). The results of the pooled OLS regression analysis show a *p*-value of the F-test which is lower than 0.05[14], and therefore significant. This means that there is a 95 per cent probability that the model has explanatory value for the e-government development, thereby rejecting the null hypothesis. The R-squared score is 0.77, which means that 77 per cent of the variance of the outcome variable e-government development is explained by the explanatory variables in the model. This means that 23 per cent of variance of the outcome variable e-government development is explained by variables which are not captured in this model. A significant *p*-value of the F-test and a relatively high R-squared score indicate that this

[14] The *alpha* value (α) for the F-test is set at 0.05 (which means a result below this value is significant). An alpha value of 0.05 is most typically used (Mehmetoglu & Jakobsen, 2017).

pooled OLS regression model fits the data well and is robust for testing the relationships between the independent variables and dependent variable.

Where the F-test focuses on the model as a whole, the t-test looks at the relationship between individual explanatory variables and the outcome/dependent variable (Park, 2011). The t-test is approached in the same way as the F-test, whereas the null hypothesis for each explanatory variable is that there is no relationship with the outcome variable.

Null hypothesis (H_0) t-test: *There is no relationship between explanatory variable X and the outcome variable.*

For this null hypothesis to be accepted, the value of the coefficient of the variable has to equal 0, whereas any value above 0 indicates the existence of a relationship between the explanatory variable and the outcome variable, and the null hypothesis would be rejected. The results of the t-tests within the pooled OLS regression analysis show that there is no explanatory variable with a t-test score or coefficient that equals 0. Hence, the null hypotheses for the t-tests are rejected, indicating the existence of a relationship between all the explanatory variables and outcome variable e-government development. The alternative hypothesis is that there is a significant relationship between the explanatory variable and the outcome variable e-government development (as presented in paragraph 3.3). The *p*-value of each t-test indicates the significance of these relationships, with a significant result for $p < 0.05$[15]. The results (see table 3) show a significant relationship between e-government development and two independent variables. The independent variables 'legal' and 'technical' have a significant association with e-government development, as for these variables $p < 0.05$. For these variables, the alternative hypothesis is accepted. This means that there is a 95 per cent probability that 'legal' and 'technical' are predictive variables for e-government development. For the independent variables 'organisational', 'capacity-building' and 'cooperation', $p > 0.05$ meaning that there is no significant relationship between these variables and e-government development. The alternative hypotheses for these variables are rejected.

Regarding the control variables, which were included as explanatory variables in the model, the results show a significant relationship between 'innovation' and e-government development because $p < 0.05$. For this variable, the alternative hypothesis is accepted. This means that there is a 95 per cent probability that 'innovation' is a predictive variable for e-government

[15] The *alpha* value (α) for the t-test is set at 0.05. An alternative value could be $\alpha = 0.1$.

development. The control variables 'national income', 'corruption' and 'state of democracy' have *p*-values higher than 0.05 and have therefore no significant relationship with e-government development. For these variables, the alternative hypotheses are rejected. What is interesting to note is that the control variable 'corruption' has a significant relationship with e-government development, would the alpha value have been set at 0.1 (α = 0.1, see table 6).

For the variables that have shown to have a significant relationship with e-government development (i.e. legal, technical and innovation), it is interesting to look at the nature of this relationship, reflected by the coefficient. The coefficients of all three significant explanatory variables are positive, which means the relationship between these variables and e-government development is positive in nature. The coefficient for 'legal' is 0.11, meaning that a 1 unit increase of 'legal' results in a 0.11 increase in e-government development. The coefficient for 'technical' is 0.115, meaning that a 1 unit increase of 'technical' results in a 0.115 increase in e-government development. The coefficient for 'innovation' is 0.011, meaning that a 1 unit increase of 'innovation' results in a 0.011 increase in e-government development.

In conclusion, the results of the pooled OLS regression analysis show a significant positive relationship between the 'legal' and 'technical' components of cybersecurity and e-government development. This means that hypothesis 1 (the *legal* component of cybersecurity has a positive relationship with the development of e-government) and hypothesis 2 (the *technical* component of cybersecurity has a positive relationship with the development of e-government) of this study are accepted. Furthermore, there is no significant relationship between the 'organisational', 'capacity-building' and 'cooperation' components of cybersecurity and e-government development. This means that hypothesis 3 (the *organisational* component of cybersecurity has a positive relationship with the development of e-government), hypothesis 4 (the *capacity-building* component of cybersecurity has a positive relationship with the development of e-government) and hypothesis 5 (the *cooperation* component of cybersecurity has a positive relationship with the development of e-government) of this study are rejected. Additionally, the analysis has found a significant positive relationship between innovation and e-government development.

To conclude, and answer this study's fourth and fifth sub-question, e-government development, cybersecurity as a whole, as well as the individual components of cybersecurity are normally distributed in a global context. There is a significant association between the combined explanatory factors within the model and e-government development, as well as between the ‘legal’ and ‘technical’ components of cybersecurity and e-government development.

Table 6 | Results pooled OLS regression analysis

Dependent variable		E-Government development
F (9, 250)		93.3
Prob > F		0.0000**
R-squared		0.77
Independent & control variables		
Legal	Coefficient Standard error t P > | t |	0.110 0.028 3.910 0.000**
Technical	Coefficient Standard error t P > | t |	0.115 0.038 3.010 0.003**
Organisational	Coefficient Standard error t P > | t |	-0.063 0.039 -1.620 0.106
Capacity-building	Coefficient Standard error t P > | t |	0.045 0.040 1.130 0.258
Cooperation	Coefficient Standard error t P > | t |	0.035 0.044 0.800 0.427
National income (GNI)	Coefficient Standard error t P > | t |	$-3.96 \cdot 10^{-15}$ $3.79 \cdot 10^{-15}$ -1.040 0.298
Corruption	Coefficient Standard error t P > | t |	0.001 0.001 1.690 0.091*
Innovation	Coefficient Standard error t P > | t |	0.011 0.001 9.490 0.000**
State of democracy	Coefficient Standard error t P > | t |	0.003 0.005 0.67 0.506
Cons	Coefficient Standard error t P > | t |	-0.222 0.223 -0.970 0.333

* Significant result when α = 0.1

** Significant result when α = 0.05

6 Discussion

Chapter 6 will consist of the interpretation of the results presented in the previous chapter, and an analysis of these results in light of earlier research (paragraph 6.1).This will give more insight in the answers to the hypotheses formulated in chapter 3 and will help answer the last sub-question of this study: 6) c*an the theoretical relationship between cybersecurity and e-government development be confirmed in a global context?* Subsequently, paragraph 6.2 will elaborate on the validity and reliability of this study, after which the implications of this study will be discussed in paragraph 6.3.

Chapter 2, 3 and 5 of this study have answered the first five sub-questions. These chapters have concluded that; 1) many factors among which corruption, innovation, national income and cybersecurity could be associated with the development of e-government; 2) the highly ambiguous concept of cybersecurity consists of the components 'legal', 'technical', 'organisational', 'capacity-building' and 'cooperation'; 3) there is, according to the literature, a positive relationship between (the individual components of) cybersecurity on the one hand and e-government development on the other; 4) that the variables in the model are normally distributed, that the model has explanatory power as a whole and that two cybersecurity components are significantly associated with e-government development.

6.1 Theoretical relationships

The pooled OLS regression analysis, of which the results are presented in chapter 5, shows the relationship between cybersecurity and e-government development, and more specifically, the relationship with the individual cybersecurity components and e-government development. The model of all explanatory variables (independent variables and control variables) proved to be powerful and robust in terms of explanatory value, as shown by the relatively high R-squared score. The hypothesised explanatory variables can to a large extent explain the variance of the outcome variable, e-government development.

More specifically, the analysis indicates a significant relationship between two of the components of cybersecurity and e-government development: 'legal' and 'technical'. This relationship entails that the legal and technical component of cybersecurity are positively associated with the development of e-government based on a panel dataset including 193 countries and 2 time periods (2014 and 2016). These results are in line with the theory and hypotheses 1 and 2, which are therefore accepted. Despite these significant relationships, the relatively low internal validity of this study, which is inherent to this type of research design, withholds the drawing of conclusions on the causality of these relationships. Notwithstanding this, the results of this study confirm the necessity of country-level legislation and regulation regarding cyber-related (illicit) behaviour for the development of e-government, as proposed in studies by Karake-Shalhoub and Al Qasimi (2010), and Alharbi, Papdaki and Dowland (2017). Additionally, the results confirm earlier claims made in studies by Verkijika and De Wet (2016), Khanyako and Maiga (2013) and Conklin (2007), that a technically resilient digital infrastructure is a prerequisite for a country's e-government development. These results show how the legal and technical components of cybersecurity are significantly associated with e-government development, representing the more 'hard' side of cybersecurity, in the shape of laws and regulations (legal component) and, information security/CIRTs (technical component), which is according to Jang-Jaccard and Nepal (2014) the least ''human' factor of cybersecurity.

Additionally, no significant relationship was found between the other three components of cybersecurity and e-government: 'organisational', 'capacity-building' and 'cooperation'. Since these variables are unable to explain the variance in e-government development among national governments around the world to an extent that is deemed significant, hypotheses 3, 4 and 5 are rejected. The disconfirmation of these relationships goes against claims made by earlier studies which indicated a positive relationship between the 'organisational' component of cybersecurity (Burns & Robins, 2003; Ebrahim & Irani, 2005; Lenk & Traunmuller, 2000; Li & Stevenson, 2002), the 'capacity-building' component of cybersecurity (Ebrahim & Irani, 2005; Heeks, 2001; Norris, Fletcher & Holden, 2001; Sarrayrih and Sriram, 2015) and the 'cooperation' component of cybersecurity (Ndou, 2004) on the one hand, and e-government development on the other. What is interesting to note here, is that all these studies underline the more 'soft side' or 'human side' of cybersecurity. A notable difference between the for e-government development significant and non-significant components of cybersecurity in this study, is the different sides ('hard' side and 'soft' side) or doctrines (explained in paragraph 2.2) of cybersecurity with which they predominantly relate. The independent variables in non-significant relationships are all more related to the newer, more socio-economic and human side of cybersecurity, as described by for instance Ashenden, Coles-Kemp and O'Hara (2018) and Salminen & Hossain (2018) to be a very important counter-balance against the technical side from which cybersecurity is mostly looked at. Their perspective falls within the doctrine public of cybersecurity created by Mulligan and Schneider (2011) which emphasises the more political and human (i.e. societal) factors to be important in cybersecurity. The aforementioned studies that found a positive relationship between the ‘organisational’, ‘capacity-building’ and ‘cooperation’ component of cybersecurity and e-government development follow this doctrine by stressing the importance of these political, human and socio-economic factors for the development of e-government. While this may be the case, this political, human and socio-economic side of cybersecurity is not associated with the development of e-government, as the results of this study show. Instead, the results of this study support the older doctrines concerning cybersecurity from the 20th century, which focus on the importance of the ‘hard’ side of cybersecurity, in the shape of laws & regulation and technological aspects.

Furthermore, the analysis found a significant positive relationship between the control variable ‘innovation’ and the development of e-government. This means that, in accordance with earlier studies by Anthopoulos, Reddick, Giannakidou and Mavridis (2015) and Verkijika and De Wet (2016), countries with a high level of innovation appear to be open for, and investing in developing electronic government systems. This seems a self-evident relationship since a large part of innovation consists of technological innovation, of which e-government is an example (Anthopoulos, Reddick, Giannakidou and Mavridis, 2015). This study confirmed the strength of this relationship. However, this is not the case for the other control variables. Regarding corruption, a positive relationship has been found, although not significant (the relationship would be significant if the alpha (α) would have been set at 0.1). This study therefore confirms the positive relationship between corruption and e-government, development, as established in earlier studies such as by Verkijika & De Wet, 2016, just not at a significant level. As many previous studies have conceptualised the relationship between corruption and e-government development slightly differently (Aladwani, 2016; Khan & Krishan, 2019; Singh, Das & Joseph, 2007: Verkijika & De Wet, 2016) this relationship would be a relevant topic for future research. Surprisingly, the control variable ‘national income’ has no significant relationship with e-government development at all. So unlike the previous studies by Verkijika and De Wet (2016) and the UN (Hafeez & Sher, 2006) have claimed, the national income of a country, which is an indicator for economic progress, is not associated with the development of e-government. This is also the case for ‘state of democracy’. Since no significant relationship has been found between this control variable and the development of e-government, this study opposes the results of the previous study by Kabanov and Sungurov (2016), which found democratic regime to be a predictor for e-government maturity.

Figure 9 shows the conceptual model of this study, with an overview of the accepted and rejected hypotheses.

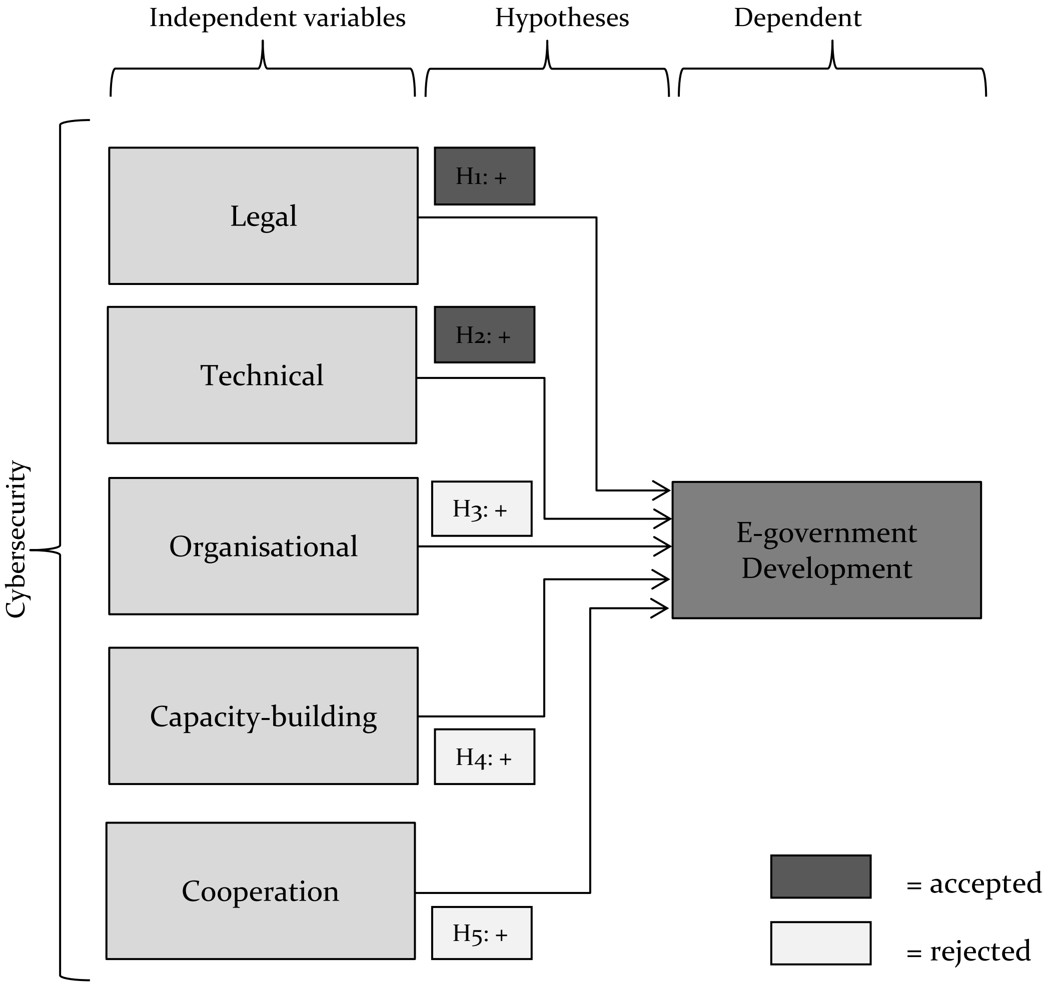

Figure 14 | Conceptual model with accepted and rejected hypotheses

Considering all the above, one can conclude that the theoretical relationships between the hard/rigid components of cybersecurity (legal and technical) and e-government development are confirmed, as well as the most technology-related control variable, innovation. On the other hand, the relationship between the more human/socio-economic and political components of cybersecurity and e-government development cannot be confirmed, unlike what was expected. Completely contrary to this new 'cybersecurity paradigm' described by Mulligan and Schneider (2011), Ashenden, Coles-Kemp and O'Hara (2018) and Salminen & Hossain (2018), this emphasises the importance of the 'hard-core' aspects for cybersecurity, at least for the development of e-government. There is also no significant relationship between national income as an indicator of economic progress, or state of democracy, and e-government development. Consequently of the near-significant relation that was found between corruption and e-government development, more research would be needed to confirm or disconfirm this relationship.

6.2 Validity and reliability

When conducting social science research, there should be attention for the *rigour* of the study, meaning the degree of quality of the research methodology (Heale & Twycross, 2015). The quality of research methodology is achieved and measured by the concepts of *validity* and *reliability* (Heale & Twycross, 2015).

6.2.1 Validity

In its purest definition, validity refers to 'truth' and 'correctness' (Kvale, 1995). In social science research, this means that validity pertains to whether the methods used in the study actually investigate what is intended to be investigated, i.e. whether the observations correctly reflect the phenomena of interest (Kvale, 1995). When it comes to quantitative social science or economic research, four types of validity are most important to take into account: statistical conclusion validity, internal validity, construct validity and external validity (Drost, 2011; Roe & Just, 2009).

There are a number of threats to statistical conclusion validity, of which the most relevant ones for this study are violation of assumptions and low statistical power (Drost, 2011). Before performing the pooled OLS regression analysis, all regression assumptions were tested to check for violations of assumptions. Where violations of assumptions were found, they were controlled for (see paragraph 4.2.3). A low statistical power can occur when for example the sample size is too small (low *n*) (García-Pérez, 2012). This study has a moderately high *n*, and the results of the pooled OLS regression analysis show a significantly strong explanatory power of all combined independent and control variables in the model for the dependent variable. This enables the possibility of finding significant results for the separate assumed relationships in the conceptual model and increases the statistical conclusion validity.

Secondly, internal validity can be described as "the ability of a researcher to argue that observed correlations are causal" (Roe & Just: p. 1266). Connected to that, internal validity refers to whether the chosen independent variables are actually predictive variables for the dependent variable and whether there are no confounding variables in the study (Drost, 2011). In this study, the data is obtained through external existing databases, which combined form the panel dataset. This means this study is restricted to the availability of quantitative data through other sources, unable to control for validity and measurement errors in the research behind these data. This severely decreases the internal validity of this study. By the inclusion of control variables, the threat of spurious effects caused by confounding unobserved variables can be minimised. The results of the pooled OLS regression analysis indeed show a relatively high R-squared score (see chapter 5), meaning that the research model has explanatory value and can thus explain variation. Even though this increases the internal validity, this study cannot argue the causality of the relationships between the variables. Despite a high R-squared score, there are still unobserved underlying variables which affect e-government development. These spurious effects are an inherent weakness of pooled OLS regression analyses (Mehmetoglu & Jakobsen, 2017). Figure 2 shows how spurious effects can occur.

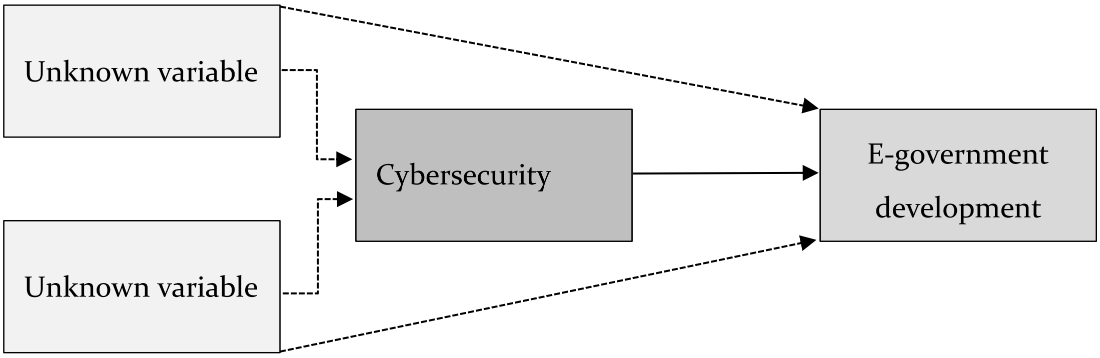

Figure 15 | Spurious effects (Mehmetoglu & Jakobsen, 2017)

Construct validity focuses on how well the abstract ideas or concepts are transformed into a concrete operating reality, i.e. the operationalisation (Drost, 2011). For the operationalisation of the concepts in this study, the indicators and their definitions are directly derived from the organisations behind the various databases. The operationalisation is therefore already conducted by the various studies behind the data, which causes this study to be dependent on the construct validity of these preceding studies. Since the used databases are commonly accepted and frequently used in academic research into the same concepts, their construct validity is assumed sufficient in this study. An important limitation concerning construct validity lays in the fact that the research behind Global Cybersecurity Index (GCI) included a number of indicators divided over the 5 pillars, into the 2016 research, which were not included in the 2014 version. A thorough investigation of the construct validity within the research behind every indicator was not feasible due to the time constraints of this research.

External validity refers to whether the relationship(s) between concepts found in the study can be generalised to a different context (e.g. time or location) (Roe & Just, 2009). To determine the external validity of this study, a number of factors have to be take into account. First, in this study it is attempted to include as many countries possible, for as many time periods as possible, which would increase the external validity. Due to constraints caused by the availability of data for the variables, the number is time periods had to be restricted to two years. Because of missing observation for at least one variable in these two time periods, the number of total observations had to be restricted to 269 (n = 269). The relatively low amount of time periods but high amount of included countries means that external validity connected to time (time-series) is low, while external validity connected to location (cross-sectional) is high. The characteristics of the panel dataset increase the possibility for cross-sectional generalisation of the results of the study, but make temporal generalisation more difficult. According to many authors, panel data studies inherently increase external validity because of increased sample size, and the ability to control for control variables, test for heteroscedasticity and examine complex conceptual models (Gil-Garcia & Puron-Cid, 2015; Hsiao, 2007; Mehmetoglu & Jakobsen, 2017). Consequently, panel data studies have a higher external validity vis-à-vis time-series or cross-sectional studies, albeit conclusions regarding causality remain impossible.

6.2.2 Reliability

The degree of reliability of a study is determined by whether repeatedly conducting the same study, yields the same results every time (Babbie, 2013). More specifically, completely reliable research should be able to be repeated by different people, in different times, under different conditions, and even with different instruments, as long as the same concept or phenomenon is investigated (Drost, 2011). The two major concerns regarding reliability are systematic errors (repeated consistent faulty measurements) and random errors (random faulty interpretations/processing of measurements) (Drost, 2011). Because this study makes use of many previously done studies for its variables, there is 1) a high chance of systematic and random errors throughout the vast amount of indicators and measurements in the research behind the combined panel dataset, and 2) no way of checking and controlling for these errors within the scope of this study. Because these measurement errors can occur in the research behind the used databases, a potential deficiency of measurement might emerge (George & Pandey, 2017). Hence, the reliability of this study is heavily dependent on the reliability of the studies conducted by the organisations behind the chosen databases: the UN, the ITU, the World Bank, Transparency International and WIPO/Cornell University/INSEAD. An example of this dependency is the inconsistency in the indicators over the two different editions of the GCI, which decreases the overall reliability, but is unfortunately inescapable. A side effect of the acceptance of this common source bias (CSB) is the uncritical acceptance of data collected through research and by researchers of which there is no control over the due diligence to assess the validity and reliability (George & Pandey, 2017). Nevertheless, while a methodological change within the GCI decreases the overall reliability, the change itself is positive for the reliability. This is because the use of binary answer system for the question in the GCI survey helps eliminate opinion-based evaluation and any possible bias towards certain types of answers (ITU, 2017). The UN EGDI uses existing UN and World Bank data for their sub-indexes HCI and TII. For the OSI, they use a survey, which is therefore susceptible to CSB. However, the UN attempts to increase reliability as much as possible, by rigorous training for the UNVs and by using a similar binary question set-up for the survey as the ITU uses (from the 2017 GCI onwards). These methodological practices increase the reliability of the studies behind the used databases, but still do not provide a researcher using these databases, the possibility to control for CSB and complete reliability. For that, the use of self-reported data is necessary (George & Pandey, 2017).

The only reliability that *can* be controlled for in this study, is the reliability of the conceptual model. The results of testing the regression assumptions showed that the variables in the model are normally distributed and have no or multicollinearity. There were also no influential outlier observations. The model has heteroscedasticity, for which was controlled in the analysis (see paragraph 4.2.3).

6.3 Implications

6.3.1 Scientific implications

This study adds to the body of literature, by addressing the gap in the literature concerning the relatively new concepts of 'cybersecurity and 'e-government' and the relationship between them. The finding of significant relationships between the 'legal' and 'technical' component of cybersecurity, while not finding this for the 'organisational', 'capacity-building' and 'cooperation' component, has two major scientific implications. Firstly, this study affirms the need for a multifactor approach concerning cybersecurity when examining its relationship with e-government development. The complexity and ambiguity of the concept of cybersecurity is extensively elaborated on in chapter 2, and the results of this study confirm that it is worthy and necessary to examine the various elements this broad concept encompasses as well as their relationship with other factors such as e-government development. Secondly, this study addresses this specific gap in the literature resulting from the lack of a multifactor approach toward cybersecurity, by examining the relationship five individual constituents of cybersecurity have with the development of e-government. Finding two significant relationships, but also *not* finding three significant relationships where they were expected, sheds light on what the relationship between cybersecurity and e-government development exactly entails and therefore provides better understanding of this relationship. These findings also provide direction for future research.

6.3.2 Future research

While this study has provided a better understanding of the relationship between cybersecurity and e-government, more profound research is needed. First and foremost, this study should be repeated as soon as the full data of the 2018 edition of the GCI are available. The addition of a third time period (2018) will provide more observations, hence a higher *n* and increased external validity. Additionally, it would provide an increased internal validity since the methodology of the research behind the 2016 and 2018 GCI would then be exactly the same, whereas the methodology of the two editions of the GCI used in this study (2014 and 2016) differ.

Secondly, this study has examined the relationship between the components of cybersecurity and e-government development as a whole. As explained in chapters 2 and 4, the concept of e-government development consists of several parts, which are separately examined in previous studies such as by Verkijika and De Wet (2016) and of which the UN provides the data, next to every country's overall e-government development score. This makes it interesting and relevant for future research to look at the relationships the separate components of cybersecurity have with the separate components of e-government development. This would give an even more detailed insight into the relationship between these two overarching phenomena.

Thirdly, this study has taken cybersecurity as independent variable and e-government development as dependent variable. In some earlier studies, such as by Onumo, Cullen and Ullah-Awan (2017), the relationship was reversely conceptualised. There seems to be a lack of consensus on the underlying theoretical relationship. When looking at the even broader concepts of 'security' and 'development' there seems to be a nexus between the two, meaning that there would be a reciprocal relationship (see chapter 3). Several authors emphasise the existence of such a nexus (Chandler, 2007; Duffield, 2010; Stern & Öjendal, 2010; Stewart, 2005). Studies such as the one by Onumo, Cullen and Ullah-Awan (2017), Verkijika and De Wet (2016) and this one, can only prove a correlation/relationship between factors, but no causality or direction of correlation. Broad and profound (qualitative) research could provide clarity on the theoretical underpinning behind the concepts of cybersecurity and e-government development and shed more light on the potential existence of a 'digital security-development nexus'.

Fourthly, this study has exclusively examined e-government development, excluding e-participation and e-democracy, which can be categorised as e-governance. Many studies including e-government or e-governance look (also) at the explanatory factors for the *adoption* and *usage* of electronic government services, hence taking on a user/citizen perspective (Alharbi, Papadaki & Dowland, 2017; Bélanger & Carter, 2009; Chourdie & Dwivedi, 2005; Colesca & Dobrica, 2008; Ebrahim & Irani, 2005; Reddick, 2005; Taipale, 2013; Van Dijk et al., 2007). The UN publishes the UN e-participation index as supplementary index to the EGDI, which would be extremely useful to examine the relationship between (components of) cybersecurity and e-governance. This is especially interesting because it would contribute to the body of knowledge on New Public Governance (NPG), whereas this study remains in the realm of New Public Management (NPM), to which e-government mostly relates.

6.3.3 Policy implications

This study shows the way in which cybersecurity is related to the development of e-government, by differentiating between the different components of cybersecurity. The results have substantial policy implications, especially because the construction and maintenance of online public services is becoming an increasingly large part of modern public administration, even though relatively little is known about what affects its successful development and implementation (Torres, Pina & Royo, 2005). Additionally, the increasing expansion of activities by governments (and society as a whole) into the digital realm, poses a higher digital vulnerability and increased cyber risks (Pupillo, 2018). This is shown by cyber-attacks on for instance the networks of the Democratic Party in the USA in 2016, the Ukrainian power grid in 2015 and the British National Health Service in 2017. These instances show the importance of cybersecurity for the online activities of public institutions. The results of this study, which show a significantly strong relationship between e-government development and only two out of the five main components of cybersecurity with, provides direction for policy makers and public sector organisations as to what cybersecurity aspects to focus on for the successful development of e-government services. Additionally, another consequence of increased online activity by governments is the need for protection of fundamental rights, democracy and the rule of law in cyberspace, something also emphasised in the EU cybersecurity strategy (European Commission, 2013). Large scale cyber threats to governments undermine these core public values as well as good governance, which are essential for the achievement of the Sustainable Development Goals (United Nations, 2019b). To guarantee the protection of these public values in the digital realm, as well as the continuity of e-government services, robust and resilient digital infrastructure needs to be at the base of e-government (United Nations, 2018). Insight in the particularities of the relationship between cybersecurity and e-government development, as provided by this study, can assist governments in creating adequate digital foundations necessary for a secure provision of online public services, the protection of core human rights and good (digital) governance as a whole.

7 Conclusion

The starting point of this study was the interrelatedness of two phenomena which —because of technological development— have emerged over the last few decades, namely cybersecurity and e-government. This study revolved around answering the following main research question: *what is the relationship between cybersecurity and e-government development, in a global context?* To answer this research question, this study sought to identify various components of the concept of cybersecurity, and assess their individual relationship with the development of electronic government services within a global outlook. By using existing data on cybersecurity and e-government development of 193 countries and over 2 separate years, this study was able to conduct a pooled OLS regression analysis, which provided insight in this relationship.

The results of this analysis confirm the relationship between two components of cybersecurity and e-government development. In accordance with the first two hypotheses, which were based on literature, this study has found a significant positive relationship between the 'legal' and 'technical' components of cybersecurity and the development of e-government. Additionally, no significant relationship was found between the development of e-government and the 'organisational', 'capacity-building' and 'cooperation' component of cybersecurity, resulting in the rejection of the last three hypotheses of this study. The positive relationships between these three components of cybersecurity and e-government development, which were expected based on the literature, can therefore not be confirmed.

Considering these results, it can thus be concluded that there are differentiated relationships between the various components of cybersecurity and the development of e-government, in a global context. Where there is a positive relationship between the 'legal' and 'technical' component of cybersecurity with e-government development, this cannot be concluded for the 'organisational', 'capacity-building' and 'cooperation' components. These conclusions contribute to the understanding of the relationship between cybersecurity and e-government. This in turn adds to the scientific discussion in the literature, not only about these two concepts, but also about the more abstract underlying concepts of 'security' and 'development'. For policymakers and public sector entities, the results provide insight in the specific cybersecurity determinants that can play a vital role in not just providing online governmental services, but also protecting critical infrastructure, ensuring good governance and upholding core human rights while doing so.

Bibliography

Aladwani, A. M. (2016). Corruption as a source of e-Government projects failure in developing countries: A theoretical exposition. *International Journal of Information Management*, *36*(1), 105-112.

Alharbi, N., Papadaki, M., & Dowland, P. (2017). The impact of security and its antecedents in behaviour intention of using e-government services. *Behaviour & Information Technology*, *36*(6), 620-636.

Ali, M. A., Hoque, M. R., & Alam, K. (2018). An empirical investigation of the relationship between e-government development and the digital economy: the case of Asian countries. *Journal of Knowledge Management*, *22*(5), 1176-1200.

Anthopoulos, L., Reddick, C., Giannakidou, I., & Mavridis, N. (2015). E-government as an Innovative product: Theories and Case Study. In C. Reddick & L. Anthopoulos (Eds). *Information and Communication Technologies in Public Administration.* (2015). Broken Sound Parkway, NW: CRC Press

Arduini, D., Denni, M., Lucchese, M., Nurra, A., & Zanfei, A. (2013). The role of technology, organization and contextual factors in the development of e-Government services: An empirical analysis on Italian Local Public Administrations. *Structural Change and Economic Dynamics*, *27*, 177-189.

Ashenden, D. M., Coles-Kemp, L., & O'Hara, K. (2018). Why Should I?: Cybersecurity, the security of the state and the insecurity of the citizen. *Politics & Governance*, *6*(2), 41-48.

Babbie, E. (2013). *The Practice of Social Research.* Boston: Wadsworth Cengage Learning.

Baker, E. W. (2014). A model for the impact of cybersecurity infrastructure on economic development in emerging economies: evaluating the contrasting cases of India and Pakistan. *Information Technology for Development*, *20*(2), 122-139.

Baldwin, D.A. (1997) 'The concept of security', Review of International Studies, 23, pp. 5-26.

Ball, N., & Halevy, T. (1996). *Making peace work: The role of the international development community* (Vol. 18). Overseas Development Council.

Baltagi, B. (2001). *Econometric Analysis of Panel Data*. John Wiley & Sons.

Baltagi, B. (2008). *Econometric Analysis of Panel Data*. John Wiley & Sons.

Bambauer, D. E. (2012). Conundrum. *Minnesota Law Review, 96*(2), 584–674.

Bayraktar, G. (2014, March). The new Requirement for a Fifth Dimension of war: Cyber Intelligence. In *ICCWS2014-9th International Conference on Cyber Warfare & Security: ICCWS 2014* (p. 9). Academic Conferences Limited.

BBC (2017). Cyber-attack: Europol says it was unprecedented in scale. BBC News. 13 May 2017.

Bekkers, V.J.J.M, (2003). E-government and the emergence of virtual organizations in the public sector. *Information Polity, 8,* (3/4), 89-102.

Bekkers, V. J. J. M., & Zouridis, S. (1999). Electronic service delivery in public administration: Some trends and issues. International Review of Administrative Sciences, 65(2), 183–196

Bélanger, F., & Carter, L. (2009). The impact of the digital divide on e-government use. *Communications of the ACM, 52*(4), 132-135.

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. *Procedia Economics and Finance, 28,* 24-31.

Berce, J., Lanfranco, S., & Vehovar, V. (2008). E-governance a new challenge after e-government. In *Proceedings of the 8th European Conference on e-Government, Lausanne, Switzerland* (pp. 63-71).

Bernerth, J. B., & Aguinis, H. (2016). A critical review and best-practice recommendations for control variable usage. *Personnel Psychology, 69*(1), 229-283.

Bhatnagar, S. (2003). E-government and access to information. *Global corruption report, 2003,* 24-32.

Botchwey, G. (2018). E-Governance and Cybersecurity: User Perceptions of Data Integrity and Protection in Ghana.

Boyne, G. A. (2002). 'Public and Private Management: What is the Difference?' *Journal of Management Studies, 39,* (1), pp. 97-122.

Bradbury, J. (2009). Public administration. In The Concise Oxford Dictionary of Politics: Oxford University Press. [Retrieved from http://www.oxfordreference.com/ view/10.1093/acref/9780199207800.001.0001/acref-9780199207800-e-1108]

Brown, M. M., & Brudney, J. L. (2001). Achieving advanced electronic government services: An examination of obstacles and implications from an international perspective. In *National Public Management Research Conference, Bloomington, IN* (Vol. 2, pp. 143-49).

Burn, J., & Robins, G. (2003). Moving towards e-government: a case study of organisational change processes. *Logistics Information Management*, *16*(1), 25-35.

Carr, M. (2016). 'Public-private partnerships in national cyber-security strategies'. *International Affairs, 92,* (1), pp. 43-62.

Chandler, D. (2007). The security–development nexus and the rise of 'anti-foreign policy'. *Journal of International relations and Development*, *10*(4), 362-386.

Chourdie, J., & Dwivedi, Y. (2005). A survey of citizens' awareness and adoption of e-government initiatives, the 'Government Gateway': A United Kingdom perspective. In: Z. Irani, T. Elliman, & O. D. Sarikas (Eds.), Proceedings of the eGovernment Workshop '05 (eGOV05) (pp. 1–13). London: Brunel University

Colesca, S. E., & Dobrica, L. (2008). Adoption and use of e-government services: The case of Romania. Journal of Applied Research and Technology, 6(2), 204–217

Conklin, W. A. (2007, January). Barriers to Adoption of e-Government. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 98-98). IEEE.

Council of European Union (2009). "Report on the implementation of European security strategy" *European security strategy A secure Europe in a better world*. Brussels: General Secretariat of the Council. [Available at:

https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/104630.pdf]

Drost, E. A. (2011). Validity and reliability in social science research. *Education Research and perspectives*, *38*(1), 105.

Drukker, D. M. (2003). Testing for serial correlation in linear panel-data models. *The stata journal*, *3*(2), 168-177.

Duffield, M. (2010). The liberal way of development and the development—security impasse: Exploring the global life-chance divide. *Security dialogue*, *41*(1), 53-76.

Dutta, S., Lanvin, B., & Wunsch-Vincent, S. (Eds.). (2016). *The global innovation index 2016: Winning with global innovation*. Johnson Cornell University.

Economist Intelligence Unit, The (2014). Democracy Index 2014. [Available at: https://www.sudestada.com.uy/Content/Articles/421a313a-d58f-462e-9b24-2504a37f6b56/Democracy-index-2014.pdf].

Economist Intelligence Unit, The (2016). Democracy Index 2016. [Available at: http://felipesahagun.es/wp-content/uploads/2017/01/Democracy-Index-2016.pdf].

European Commission (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Security Cyberspace. [Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf].

Europol. (2018). Internet Organised Crime Threat Assessment (IOCTA). Available at: [https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018].

Ewalt, J. (2001). Theories of Governance and New Public Management: Links to Understanding Welfare Policy Implementation. Prepared for presentation at the Annual conference of the American Society for Public Administration. Newark, NJ, March 12, 2001.

Farrar, D. E., & Glauber, R. R. (1967). Multicollinearity in regression analysis: the problem revisited. *The Review of Economic and Statistics*, 92-107.

Garcia-Murillo, M. A. and Ortega, R., (2010). Do E-Government Initiatives Reduce Corruption? Available at SSRN: http://dx.doi.org/10.2139/ssrn.2012470

García-Pérez, M. A. (2012). Statistical conclusion validity: Some common threats and simple remedies. *Frontiers in psychology*, *3*, 325.

George, B., & Pandey, S. K. (2017). We know the Yin—But where is the Yang? Toward a balanced approach on common source bias in public administration scholarship. *Review of Public Personnel Administration*, *37*(2), 245-270.

Ghere, R. K., & Young, B. A. (1998). The cyber-management environment: Where technology and ingenuity meet public purpose and accountability. *Public Administration and Management: An Interactive Journal*, *3*(1).

Gil-Garcia, J., & Puron-Cid, G. (2015). Using panel data techniques for social science research: an illustrative case and some guidelines. *CIENCIA ergo-sum, ISSN 1405-0269*, Vol. 21-3.

Goodman, S.E., & Lin, H.S. (Eds.) (2007). *Toward a Safer and More Secure Cyberspace.* Washington DC: National Academic Press.

Gortney, W. E. (2016). *Department of defense dictionary of military and associated terms* (No. JP-1-02). Joint Chiefs of Staff Washington United States.

Greene, W. (2012). *Econometric analysis* (4th ed.). Upper Saddle River, N.J.: Prentice-Hall.

Hafeez, S. & Sher, S. (2006). UN Global E-government Readiness Report 2005: From E-government to E-inclusion. New York: United Nations.

Halchin, L. E. (2004). Electronic government: Government capability and terrorist resource. *Government Information Quarterly*, *21*(4), 406-419.

Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative studies. *Evidence-based nursing*, *18*(3), 66-67.

Heeks, R. (1998). Information systems and public sector accountability. The University of Manchester, Institute for Development, Policy and Management Information, Systems, Technology and Government: Working Papers Series, Number 1/1998. [Available at: http://idpm.man.ac.uk/idpm/isps_wp1.htm.]

Heeks, R. (2001). Understanding e-governance for development. The University of Manchester, Institute for Development, Policy and Management Information, Systems, Technology and Government: Working Papers Series, Number 11/2001. [Available at: http://idpm.man.ac.uk/idpm/igov11abs.htm.]

Homburg, V., & Bekkers, V. (2004). E-government and NPM: a perfect marriage?. In *Proceedings of the 6th international conference on Electronic commerce* (pp. 547-555). ACM.

Hood, C. (1991). A Public Management for all Seasons. Public Administration, 69(0), 3–19. doi:10.1111/j.1467-9299.1991.tb00779.x

Hughes, O. E. (2003). The traditional Model of Public Administration. In: Public management and administration: an introduction (pp. 17–32). Palgrave.

Hsiao, C. (1986). Analysis of panel data. Cambridge: Cambridge University Press.

Hsiao, C. (2007). Panel data analysis—advantages and challenges. *Test*, *16*(1), 1-22.

International Peace Academy (2004). Strengthening the Security-Development Nexus: Assessing International Policy and Practice Since the 1990s. [Available at: https://www.ipinst.org/wp-content/uploads/2015/06/strengthening_sec_dev_nexus.pdf].

ITU (2015). Global Cybersecurity Index and wellness profiles. [Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf].

ITU (2017). Global Cybersecurity Index 2017. [Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf].

ITU (2018). Global Cybersecurity Index 2018. [Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx].

Jang-Jaccard, J. and Nepal, S. (2014). 'A survey of emerging threats in cybersecurity.' *Journal of Computer and System Sciences, 80*, 5, pp. 973-993.

Kabanov Y., Sungurov A. (2016) E-Government Development Factors: Evidence from the Russian Regions. In: Chugunov A., Bolgov R., Kabanov Y., Kampis G., Wimmer M. (eds) Digital Transformation and Global Society. DTGS 2016. Communications in Computer and Information Science, vol 674. Springer, Cham

Kapila, M. and Wermester, K. (2002). "Development and Conflict: New Approaches in the UK," in: Hampson, F. O. and Malone, D. M., (eds.) *From Reaction to Conflict Prevention, Opportunities for the UN System*. London: Lynne Rienner Publishers.

Karake-Shalhoub, Z., & Al Qasimi, L. (2010). *Cyber law and cyber security in developing and emerging economies*. Edward Elgar Publishing.

Kaufmann, D., Kraay, A., & Mastruzzi, M. (2003). *Governance matters III: Governance indicators for 1996–2002*. The World Bank.

Kennedy, P. (2008*). A Guide to Econometrics*, 6th ed. Malden, MA: Blackwell Publishing.

Khan, A., & Krishnan, S. (2019). Conceptualizing the impact of corruption in national institutions and national stakeholder service systems on e-government maturity. *International Journal of Information Management*, *46*, 23-36.

Khanyako, E., & Maiga, G. (2013, May). An information security model for e-government services adoption in Uganda. In *2013 IST-Africa Conference & Exhibition* (pp. 1-11). IEEE.

Kickert, W. (1997). Public Management in the United States and Europe. In: W.J.M. Kickert (ed): Public Management and Administrative Reform in Western Europe, Edward Elgar, London, 1997, pp. 15-38.

Kim, C. K. (2007). A Cross-national Analysis of Global E-government. *Public Organization Review*, *7*(4), 317-329.

Kim, H., Pan, G., & Pan, S. (2007). Managing IT-enabled Transformation in the Public Sector. A case study of e-government in Korea. *Government Information Quarterly*, *24*, 338 – 352.

Koops, B. (2011). 'The Internet and its Opportunities for Cybercrime' *Tilburg Law School Legal Studies Research Paper Series* No. 09/2011, pp. 735-754

Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime, Law and Social Change*, *66*(3), 313-338.

Kvale, S. (1995). The social construction of validity. *Qualitative inquiry*, *1*(1), 19-40.

La Porte, T. M., De Jong, M., & Demchak, C. C. (1999). Public organizations on the World Wide Web: Empirical correlates of administrative openness. [Available at: http://www.cyprg.arizona.edu/publications/correlat.rtf.]

Lee, Y. (2017). Exploring the relationship between E-government development and environmental sustainability: A study of small island developing states. *Sustainability*, *9*(5), 732.

Lenk, K., & Traunmuller, R. (2000). A framework for electronic government. In *Proceedings 11th International Workshop on Database and Expert Systems Applications* (pp. 271-277). IEEE.

Li, F. (2003). Implementing E-Government strategy in Scotland: current situation and emerging issues. *Journal of Electronic Commerce in Organizations (JECO)*, *1*(2), 44-65.

Li, Z., & Liao, Q. (2018). Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. *Government Information Quarterly*, *35*(1), 151-160.

Lips, A. M. B., & Schuppan, T. (2009). Transforming e-government knowledge through public management research. *Public Management Review, 11*(6), 739-749.

Lupu, D., & Lazăr, C. G. (2015). Influence of e-government on the level of corruption in some EU and non-EU states. *Procedia Economics and Finance*, *20*, 365-371.

Máchová, R., Volejníková, J., & Lněnička, M. (2018). Impact of E-government Development on the Level of Corruption: Measuring the Effects of Related Indices in Time and Dimensions. *Review of Economic Perspectives*, *18*(2), 99-121.

Matthews, B., & Ross, L. (2010). *Research methods*. Pearson Higher Ed.

Mayer-Schönberger, V., & Hurley, D. (2000). Globalization of Communication. In: Nye, J. S., & Donahue, J. D. (Eds.). (2000). *Governance in a globalizing world*. Brookings Institution Press.

McGregor, E. B., Jr. (2001). Web page accountability: The case of public schools. Paper presented at the National Public Management Research Conference, Bloomington, IN.

Means, G., & Schneider, D. (2000). *Meta-capitalism: the e-business revolution and the design of 21st century companies and markets.* New York: John Wiley & Sons Inc.

Mehmetoglu, M., & Jakobsen, T. (2017). *Applied statistics using Stata, a guide for the social sciences.* Londen, California, New Delhi, Singapore: Sage.

Mistry, J. J., & Jalal, A. (2012). An empirical analysis of the relationship between e-government and corruption. *The International Journal of Digital Accounting research, 12*(18), 145-176.

Muller, L. P. (2015). Cyber security capacity building in developing countries: challenges and opportunities. Oslo: Norwegian Institute for International Affairs.

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for cybersecurity. *Daedalus*, *140*(4), 70-92.

Mulrow, C. D. (1994). Systematic reviews: rationale for systematic reviews. *British Medical Journal*, *309*(6954), 597-599.

Nam, T. (2018). Examining the anti-corruption effect of e-government and the moderating effect of national culture: A cross-country study. *Government Information Quarterly*, *35*(2), 273-282.

Ndou, V. (2004). E–Government for developing countries: opportunities and challenges. *The electronic journal of information systems in developing countries*, *18*(1), 1-24.

Norris, D. F., Fletcher, P. D., & Holden, S. H. (2001). Is your local government plugged in? Highlights of the 2000 electronic government survey. *Washington, DC: International City/County Management Association*.

Onumo, A., Gullen, A., & Ullah-Awan, I. (2017). Empirical study of the impact of e-government services on cybersecurity development. In *2017 Seventh International Conference on Emerging Security Technologies (EST)* (pp. 85-90). IEEE.

Orelli, R. L., Padovani, E., & del Sordo, C. (2013). From E-Government to E-Governance in Europe. In *From Government to E-Governance: Public Administration in the Digital Age* (pp. 195-206). IGI Global.

Organisation for Economic Co-operation and Development. (2012). *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*. OECD Publishing.

Osborne, S.P. (2006). 'The New Public Governance?' *Public Management Review, 8,* (3), pp. 377–387.

Park, D. W. (2016). Analysis and Comparison of Regulations for National Cybersecurity. *International Journal of Security and Its Applications*, *10*(10), 207-214.

Park, H. M. (2011). Practical guides to panel data modeling: A step by step analysis using Stata. *Public Management and Policy Analysis Program, Graduate School of International Relations, International University of Japan*, 1-52.

Patyal, M., Sampalli, S., Ye, Q., & Rahman, M. (2017). Multi-layered defense architecture against ransomware. *International Journal of Business and Cyber Security*, *1*(2).

Pupillo, L. (2018). EU Cybersecurity and the Paradox of Progress. *CEPS Policy Insight*, (2018/06).

Reddick, C. G. (2005). Citizens interaction with e-government: From the streets to server? Government Information Quarterly, 22, 38–57.

Roe, B. E., & Just, D. R. (2009). Internal and external validity in economics research: Tradeoffs between experiments, field experiments, natural experiments, and field data. *American Journal of Agricultural Economics*, *91*(5), 1266-1271.

Salminen, M., & Hossain, K. (2018). Digitalisation and human security dimensions in cybersecurity: an appraisal for the European High North. *Polar Record*, *54*(2), 108-118.

Sarrayrih, M. A., & Sriram, B. (2015). Major challenges in developing a successful e-government: A review on the Sultanate of Oman. *Journal of King Saud University-Computer and Information Sciences*, *27*(2), 230-235.

Shim, D. C., & Eom, T. H. (2008). E-government and anti-corruption: Empirical analysis of international data. *Intl Journal of Public Administration*, *31*(3), 298-316.

Singh, H., Das, A., & Joseph, D. (2007). Country-level determinants of e-government maturity. *Communications of the Association for Information Systems*, *20*, 632–648.

Siskos, E., Askounis, D., & Psarras, J. (2014). Multicriteria decision support for global e-government evaluation. *Omega*, *46*, 51-63.

Slater, M. B. (2008). Imagining numbers: Risk, quantification and the aviation industry. *Security Dialogue*, *39*(2-3), 243-266.

Sorn-In, K., Tuamsuk, K., & Chaopanon, W. (2015). Factors affecting the development of e-government using a citizen-centric approach. *Journal of Science & Technology Policy Management*, *6*(3), 206-222.

Stern, M., & Öjendal, J. (2010). Mapping the security—development nexus: conflict, complexity, cacophony, convergence?. *Security Dialogue*, *41*(1), 5-29.

Stevens, T. (2018). Global Cybersecurity: New Directions in Theory and Methods. *Politics and Governance, 6*(2), 1-4.

Stewart, F. (2004). Development and security. *Conflict, Security & Development*, *4*(3), 261-288.

Štitilis, D., Pakutinskas, P., & Malinauskaitė, I. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security Journal*, *30*(4), 1151-1168.

Sutherland, E. (2017). Governance of cybersecurity-The case of South Africa. *African Journal of Information and Communication*, *20*, 83-112.

Sutherland, E. (2018). Cybersecurity: governance of a new technology. Political Studies Association International Conference, 26-28 March 2018.

Taipale, S. (2013). The use of e-government services and the Internet: The role of socio-demographic, economic and geographical predictors. *Telecommunications Policy*, *37*(4-5), 413-422.

Tamarkin, E. (2015). The AU's cybercrime response: A positive start, but substantial challenges ahead. [Available at: https://www.africaportal.org/publications/the-aus-cybercrime-response-a-positive-start-but-substantial-challenges-ahead/].

Torres, L., Pina, V., & Royo, S. (2005). E-government and the transformation of public administrations in EU countries: Beyond NPM or just a second wave of reforms?. *Online Information Review*, *29*(5), 531-553.

Torres-Reyna, O. (2007). Panel Data Analysis. Fixed and Random Effects using Stata. [Available at: https://dss.princeton.edu/training/Panel101.pdf].

Transparency International. (2018). Corruption Perception Index 2018. [Available at: https://www.transparency.org/whatwedo/publication/corruption_perceptions_index_2018].

United Nations (2005). In larger freedom: towards development, security and human rights for all. New York: United Nations. [Available at: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/CPR%20A%2059%202005.pdf]

United Nations (2014). United Nations E-Government Survey 2014. [Available at: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf].

United Nations (2016). United Nations E-Government Survey 2016. [Available at: http://workspace.unpan.org/sites/Internet/Documents/UNPAN97453.pdf].

United Nations (2018). United Nations E-Government Survey 2018. [Available at: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018].

United Nations (2019a). UN E-Government Knowledgebase: Overview. [https://publicadministration.un.org/egovkb/en-us/Overview]. Accessed on: 13 April 2019.

United Nations (2019b). UN E-Government Knowledgebase: e-government. [https://publicadministration.un.org/egovkb/en-us/About/UNeGovDD-Framework]. Accessed on: 20 May 2019.

United Nations (2019c). UN E-government Knowledgebase: E-Government Development Index (EGDI). [https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index]. Accessed on: 20 May 2019.

United Nations & American Society for Public Administration (2002). Benchmarking E-government: A Global Perspective. New York: United Nations.

US Government (1993). Reengineering through Information Technology, National Performance Review, September, Washington, DC: Office of the Vice President. [Available at http://govinfo.library.unt.edu/npr/library/ reports/itexe.html].

Van Dijk, J., Pieterson, W., Van Deuren, A., & Ebbers, W. (2007). Services for citizens: The Dutch usage case. In: M. A. Wimmer, H. J. Scholl, & A. Grönlund (Eds.), International Conference on Electronic Government (pp. 155–166). Berlin Heidelberg: Springer-Verlag.

Verkijika, S. F., & De Wet, L. (2016). e-Government development in Sub-Saharan Africa (SSA): Relationship with macro level indices and possible implications. In *2016 IST-Africa Week Conference* (pp. 1-10). IEEE.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Wallis, J., & Zhao, F. (2018). e-Government development and government effectiveness: A reciprocal relationship. *International Journal of Public Administration*, *41*(7), 479-491.

Warner, M. (2012). Cybersecurity: a pre-history. *Intelligence and National Security*, *27*(5), 781-799.

Webster, F. (2014). *Theories of the information society*. Routledge.

West, D. M. (2004). E-government and the transformation of service delivery and citizen attitudes. *Public administration review*, *64*(1), 15-27.

Whitmore, A. (2012). A statistical analysis of the construction of the United Nations E-Government Development Index. *Government Information Quarterly*, *29*(1), 68-75.

Wolfers, A. (1952). "National Security" as an Ambiguous Symbol', *Political Science Quarterly, 67,* pp. 483.

World Bank. (2019). GNI (current US$). [https://data.worldbank.org/indicator/NY.GNP.MKTP.CD]. Accessed on: 26 May 2019.

World Bank, LAC PREM – "Issues Note: E-Government and The World Bank". November 5, 2001.

Yildiz, M. (2007). E-government research: Reviewing the literature, limitations, and ways forward. *Government information quarterly*, *24*(3), 646-665.

Zhang, H., Tang, Z., & Jayakar, K. (2018). A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services. *Telecommunications Policy*, *42*(5), 409-420.

Zhao, F., Wallis, J., & Singh, M. (2015). E-government development and the digital economy: a reciprocal relationship. *Internet Research*, *25*(5), 734-766.

Appendix: robustness tests

Because the statistical model in this study only includes two time-periods, several extra robustness checks will be represented here.

First, the two time-periods were regressed separately, of which the results are presented underneath.

2014			Number of obs.	135
			F(9, 125)	47.81
			Prob > F	0.000
			R-squared	0.77
Variable	**Coef.**	**Std. Err.**	**t**	**P> |t|**
Legal	0.142	0.036	3.97	0.000
Technical	0.096	0.058	1.67	0.098
Organisational	-0.088	0.055	-1.62	0.108
Capacity-building	0.089	0.061	1.47	0.145
Cooperation	0.056	0.079	0.70	0.483
National income	-6.35e-16	6.15e-15	-0.10	0.918
Corruption	0.001	0.001	1.46	0.146
Innovation	0.010	0.002	6.02	0.000
State of democracy	0.003	0.007	0.51	0.607

2016			Number of obs.	125
			F(9, 115)	48.67
			Prob > F	0.000
			R-squared	0.79
Variable	**Coef.**	**Std. Err.**	**t**	**P> |t|**
Legal	0.096	0.054	1.78	0.078
Technical	0.139	0.055	2.50	0.014
Organisational	-0.054	0.067	-0.81	0.418
Capacity-building	-0.013	0.057	-0.23	0.821
Cooperation	-0.021	0.056	-0.37	0.711
National income	-7.83e-15	4.69e-15	-1.67	0.098
Corruption	0.000	0.001	0.02	0.981
Innovation	0.013	0.002	7.63	0.000
State of democracy	-0.002	0.006	-0.25	0.803

In the model where the two years are combined, both IVs ‘legal’ and ‘technical’ are significantly correlated with e-government development. Regressing the two years separate shows that for 2014, ‘legal’ is significantly correlated with e-government development while ‘technical’ is not. For the year 2016, this is the other way around. The fact that combining the two years into one panel dataset results in both ‘legal’ and ‘technical’ variables to be significantly correlated with e-government development is in line with these results. The significance levels of the control variables in the tests with separate years are similar to the ones using the combined dataset.

Secondly, the regression was conducted using a dummy for individual time periods. A dummy variable was created for the year 2014 and 2016, however due to collinearity, one of these time period dummies was omitted.

Time period dummy			Number of obs.	260
			F(10, 249)	85.79
			Prob > F	0.000
			R-squared	0.76
Variable	**Coef.**	**Std. Err.**	**t**	**P> |t|**
Legal	0.127	0.029	4.38	0.000
Technical	0.097	0.039	2.48	0.014
Organisational	-0.049	0.039	-1.27	0.204
Capacity-building	0.033	0.040	0.83	0.410
Cooperation	0.007	0.046	0.15	0.880
National income	-3.79e-15	3.78e-15	-1.00	0.316
Corruption	0.001	0.001	1.22	0.223
Innovation	0.011	0.001	9.51	0.000
State of democracy	0.002	0.005	0.53	0.599
Y14 (dummy)	-0.033	0.015	-2.23	0.027

Lastly, the regression analysis was performed using a model with only the independent variables and no control variables, to check if spurious correlation can be avoided. The results are presented in the following table.

Only IVs			Number of obs.	386
			F(5, 380)	91.82
			Prob > F	0.000
			R-squared	0.55
Variable	**Coef.**	**Std. Err.**	**t**	**P> |t|**
Legal	0.241	0.031	7.69	0.000
Technical	0.172	0.048	3.61	0.000
Organisational	0.030	0.048	0.62	0.536
Capacity-building	0.067	0.051	1.31	0.191
Cooperation	0.107	0.055	1.96	0.051

The results show the same independent variables to be significantly correlated with e-government development as compared to the complete model in this study.