Copyright © 2018 International Journal of Cyber Criminology – ISSN: 0973-5089
January – June 2018. Vol. 12(1): 300–315. DOI: 10.5281/zenodo.1467929
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Governing Cyber Security through Networks: An Analysis of Cyber Security Coordination in Belgium

Rafael Rondelez[1]
Ghent University, Belgium

Abstract

While governments develop formal and informal structures or 'networks' to promote collaboration between governmental departments and agencies, there remains uncertainty on how to set up and develop cyber security networks. The latter is demonstrated when taking recent developments in the field of cyber security in Belgium into consideration. The 2012 decision to create the Belgian cyber security centre seems to entail a move towards a 'Weberian' hierarchical network coordination approach rather than the development of a cyber security network organisation. This article claims that - as the threats of cyber are becoming more complex - there is a growing need for governmental agencies to expand horizontal coordination mechanisms. From this follows, the growing demand for criminological research into the managerial aspects of cyber security networks. Generating knowledge on how to manage networks is required as the latter is not only decisive for the effectiveness and efficiency of cyber security networks but also contributes to the overall network cyber security governance.

Keywords: Belgium, cybercrime, cyber security, network forms of organisation.

Introduction

There exists a great interest amongst contemporary criminologists in analysing the pluralisation of policing and the emergence of networked approaches for governing security or controlling crime (Dupont, 2004; 2006, Flemming & Wood, 2006; Wood & Dupont, 2006).

While the concept of '*networks*' yields considerable attention in the literature, the usage of this concept remains largely driven by intuition about what a network is or how it should behave (Brewer, 2017). Many of these scholars focus on the nature and patterns of the relationships between the various network actors (Yip, 2016; Décary-Hétu & Dupont, 2012) as they are interested in studying the various ways in which information and resources flow across networks (see for example: Leukfeldt, 2016; Sabillon, Cano, Cavaller, & Serra, 2016; Leukfeldt, Veenstra, & Stol, 2013; Hunton, 2010; Lu, Luo,

[1] MSc in Criminology, Doctoral Researcher at Ghent University, St. Pietersnieuwstraat 33, 9000 Gent, Belgium. Email: rafael.rondelez@ugent.be

Polgar, & Cao, 2010). This results in theoretical assumptions being drawn about neat, highly coordinated assemblages that presuppose activities of coproduction via horizontal partnerships (Brodeur & Dupont, 2006; Dupont, 2006; Schuilenburg, 2015; Van Ryckeghem, Bruggeman, Easton, & Ponsaers, 2014).

Unfortunately, even though various scholars stress that structural factors such as '*network design*' and '*network governance*' are decisive for the overall effectiveness and efficiency of networks, only a few criminologists scrutinise the governance features of these networks to capture and explain precisely how governance serves to shape network outcomes (Whelan, 2012). Consequently, until today little attention is paid to analyse the network as 'a whole' or integrated entity (Whelan, 2012).

From this stems that '*management of networks*' or '*governance of networks*' should become the main orientation of criminological research instead of focussing - primarily - on networks as a means of networked (cyber-) security governance (Provan & Kenis, 2007).

This need for additional research also stems from the debate on how governmental agencies can increase their efficiency and effectiveness in preventing and combating cyber crime. Threats of cyber are becoming more and more complex since computer systems are increasingly embedded or interdependent and the number of cyber attacks continuously increases. Consequently, a sense of urgency for developing new security directions, guidelines and practices to counter cyber-risks worldwide raises (Hojsgaard Munk, 2015). Several governments already developed new or adapted (criminal) legislation following the signing and ratification of international agreements such as the 2001 Budapest '*Convention on Cyber crime*' (Kerkhofs & Van Linthout, 2013). Others joined forces and developed regional platforms - such as '*the European Cybercrime Centre (EC3)*' (Europol, 2017) - in view of enhancing cross-border cooperation and information exchange. However, uncertainty reigns about organisational adaptations as there remains a lack of insight about which organisation is best in the field of cyber security (Smith & Ingram, 2017).

Motivated to bridge this knowledge gap, this article envisages achieving a two-folded objective. First it provides clarity regarding the concepts: '*network governance*' and '*governance of networks'*. In addition, it outlines the move from an informal multi-disciplinary cyber security network into a more 'Weberian' oriented networked coordination mechanism.

The relevancy of this analysis is rooted in the fact that the network concept has been heralded as the way to tackle '*wicked*' (Rittel & Webber, 1973) cyber security issues more effectively and efficiently while modesty is required. The network concept does not represent '*a one fit all*' solution. Each network organisation requires a profound consideration of its design as well as the critical role of internal governance (Antivachis & Angelis, 2015; Turrini, Cristofoli, Frosini, & Nasi, 2010).

To achieve these objectives, the study applies a qualitative research design based on a literature review and a case-study. The literature review concerns the analysis of academic literature on '*network governance*' and '*governance of networks*' from different fields such as criminological, sociological, political, public management and others. The case-study entails an analysis of available government documents covering the period from the beginning of the millennium up to the end of 2016 and which are related to the development of an inter-agency cyber security capability in Belgium. The following documents are analysed: '*cyber security*'-related resolutions as submitted to the Belgium Chamber of Representatives, cyber security strategies, policy statements, the Royal decree

concerning the creation of the cyber security centre of Belgium (CCB or Centrum voor Cyber security België) from 10 October 2014, the interdepartmental brief called '*Kadernota Integrale Veiligheid 2016-2019*', the National security plan 2016-2019 (Nationaal veiligheidsplan 2016 - 2019), the Cyber security Centre of Belgium strategic plan 2015-2020 and the 2015 CCB annual report.

The research is not to be considered as a linear process. The preparation is characterised by an ongoing selection-process of identifying research areas and selecting sources. Various desktop research sessions are organised, and numerous open sources are consulted. Relevant documents are retrieved based on the following key words: Belgium, cybercrime, cyber security, policing, governance, security network and network forms of organisation. These keywords are inserted in several search engines of various online platforms e.g. Google Scholar and ResearchGate.

Faced with a broad field of research - governing cyber security - it is necessary to limit the scope of this article. It is not the aim to assess the effectiveness of the inter-agency cyber security capability in Belgium as effectiveness might be influenced by several '*endogenous*' or '*exogenous*' (Kenis & Provan, 2009) factors. Rather, this study aims to provide a more detailed insight in the recent history of cyber security governance in Belgium as to illustrate the ambiguity which remains regarding the governance of governmental networks in the domain of cyber security.

The final ambition is to deliver a contribution which holds relevancy for discussing public sector networks facing collective-action issues such as delivering cyber security where public prosecutors, law enforcement, intelligence and other governmental departments and agencies need to work together through networks. It may draw the attention of policy-makers and practitioners to the importance of analysing management contingencies against network properties, processes and outcomes. Finally, the outcome of this research may serve to improve the designing cyber security networks.

The article is structured in two parts. This introduction is followed by the first section in which conceptual aspects of network governance and the governance of networks are discussed. The second part covers the analysis of the case-study and the article is concluded with conclusion and recommendations.

1. Network Governance or Governance of Networks?

This section serves as the theoretical foundation of this paper and provides some clarity in the concepts of '*network governance*' and '*governance of networks*'. Whilst these perspectives seem to overlap, there is a substantial difference between both.

a. Network governance

Solving societal problems - such as poverty, climate change or marine pollution - is nowadays very complex or '*wicked*' due to the social complexity of these issues. As these issues have no determinable stopping point and are characterised by a complex of interdependencies, every attempt to solve one aspect of such a problem reveals or creates other issues (Rittel & Webber, 1973).

Since the introduction of digital information and communication technologies (Castells, 2000), crime and the provision of security developed a similar 'wickedness'. Consequently, the pressure increased to find alternatives for the previous applied traditional methods and instruments for policing crime and governing security (Klijn,

2012). As a result, a debate developed on the ways and extent to which hierarchical, state-led provision of security has been displaced by a move towards a '*decentred*' (Bisschop & Verhage, 2012) or polycentric - networked-oriented - mode of coordination (Yar, 2011). This transition - often called the move from '*government*' to '*governance*' - refers to the existence of multiple (public-private) police partnerships or '*security networks*' (Dupont, 2004)

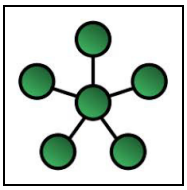
Alternatives for the old-school top-down public management or '*government*' approach (Rhodes, 1996; Charbonneau, 2012; Pollitt, 2003; Stoker, 2002) were recently developed and are now commonly referred to as the '*New Public Management*' and the '*Governance model*' perspectives. While the '*New Public Management model*' (Hood, 1991) focuses on optimizing the public sector through inter-organisational, contractual relationships based on market principles (Easton, 2015), the '*governance model*' (Rhodes, 1996; 2007) is more oriented towards trying to approach problems by applying the network concept rather than by applying market principles (Klijn, 2012).

'*Networks*' or '*network organisations*' are within this governance perspective considered as being a distinctive form of social organization or organizational structure as they not only complement but may as well result in several advantages over '*markets and bureaucratic hierarchies*' (Provan & Kenis, 2007; van Dijk & Winters-van Beek, 2009). Networks represent reciprocal arrangements of communication and exchange between autonomous but interdependent organisations which result in increased resources to address '*wicked*' issues. (Hajer, Van Tatenhove, & Laurent, 2004)

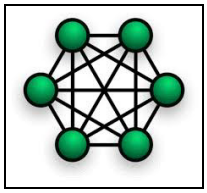
From this stems that a network or network organisation should be considered as a '*locus of production*' – like individual organisations - consisting of minimum three autonomous but interdependent legally organisations that work together to achieve a common goal rather than their own objectives and jointly produce an output or whole network (Raab & Kenis, 2009; Provan & Kenis, 2007). In addition, networks can be further categorized into '*serendipitous*' or '*networks an sich*' and '*goal-directed*' or '*networks für sich*' (Provan & Kenis, 2007). In the former category networks are considered as informal or '*emergent*' networks which are developed not by design but haphazardly (Monge & Contractor, 2003). The latter category - '*goal-directed*' networks – refers to those networks which are consciously planned and coordinated (Whelan, 2012).

Following the literature two basic network designs exist: '*hub*' (or '*star*') and '*all-channel*' or '*full-matrix*' networks (Whelan, 2012). Each design has different properties and processes, which of course affect the exchange of information and the way the network is governed '*internally*' (Provan & Kenis, 2007).

Figure 1. Basic types of network designs



Hub or star network



All-channel or full-matrix network

In a '*hub*' or '*star network*', each actor is tied to a central node or actor and must go through that node to communicate and coordinate. In the other concept, the '*all-channel*' or '*full-matrix network*', each actor is tied to every other actor.

b. The 'governance of networks' concept

The previous section demonstrated that networks are nowadays commonly used as forms of governance to address complex or wicked issues through multilateral coordination (van Dijk & Winters-van Beek, 2009).

However, networks are often created in response to an external pressure assuming that the problem for which the network is created will resolve automatically or '*an sich*' because a group of actors '*network*' and communicate in a horizontal way (Provan & Kenis, 2009).

But network governance signifies more than just achieving goals of individual organisations as the performance of the individual organisations is of less importance compared to the outcome at network level (O'Toole, 1997). '*Network outcomes*' are thus a central feature of the network governance perspective (Whelan, 2012) with '*network effectiveness*' being the most important one as it refers to the attainment of positive network level outcomes that could not normally be achieved by individual organizational participants acting independently (Provan & Kenis, 2007). The latter is however a problematic concept as it may result in '*Network Euphoria*' (Provan & Kenis, 2009). It is often taken for granted that networks represent '*a one fit all solution*' and only deliver positive outcomes which is not the case as demonstrated after the 2005 Katrina hurricane disaster in New Orleans (van Dijk & Winters-van Beek, 2009).

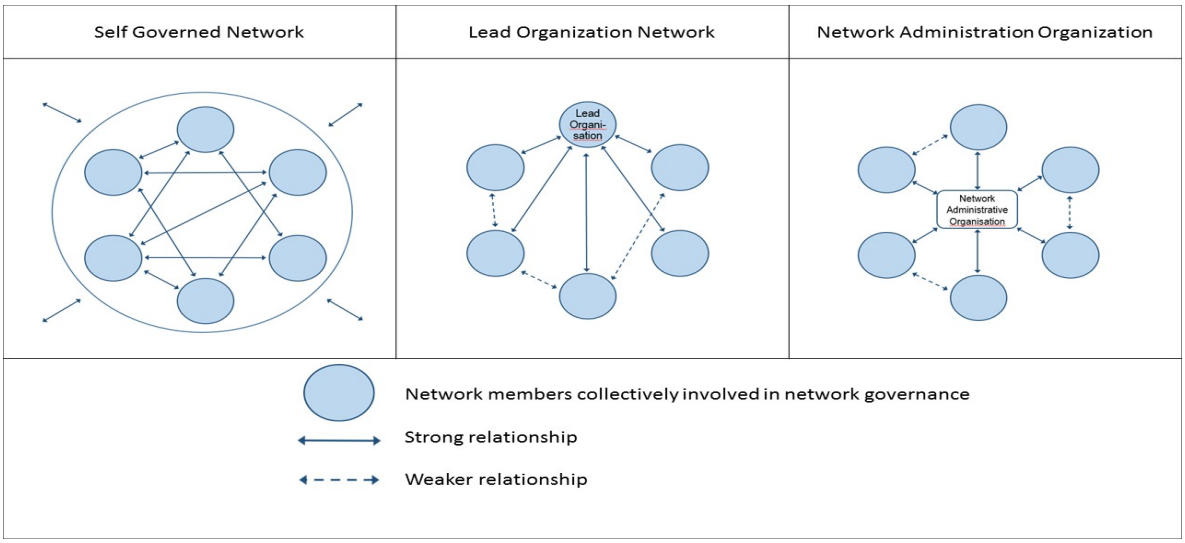
From this stems that networks require to be internally managed or governed. In the literature reference is made to the concept of '*governance of networks*' or '*internal network governance*' as it entails the coordination or management of information, resources, activities and competences of at least three organizations within a partnership or network organization with the aim of producing a joint outcome (Provan & Kenis, 2007). The lack of knowledge on how to organize internal network governance in governmental networks is, according to Kamark (2002), mainly due to the fact that only few people in government really understand how to manage security networks. Government managers manage networks based on their experience and training in managing traditional bureaucracies. Knowing how to manage networks is essential to ensure that participants within the network engage in collective and mutually supportive action and address or resolve conflicts. In addition, it is also about acquiring resources or executing control and verifying whether these resources are utilized efficiently and effectively.

This brings us to the fact that internal network governance can be categorized according to two different dimensions: '*all-shared*' or '*brokered*' (Provan & Kenis, 2007).

The first type of governance concerns the '*participant governance*' or '*self-governed network*' (Provan & Kenis, 2007). Within this type there is no formal organ that drives actors from above. There is a shared responsibility between partners though specific responsibilities can be taken up by one actor. Thus, the structure depends strongly on the participation of actors (Agranoff & McGuire, 2007; Provan & Kenis, 2007). The second type of internal network governance consists of 'lead organization-governed networks'. These networks represent a more centralized form of governance in which one core

player within the network takes the lead. The core player acquires its leading position often because of its availability or contribution to more specific forms of - e.g. monetary, political or symbolic - '*capital*' (Dupont, 2004; 2006). The function of the lead organization is to facilitate the other actors in their actions (Agranoff & McGuire, 2007; Provan & Kenis, 2007). In the '*network administrative organization*' type of network, the core of the governance power is not located within the network but within an external unit. The external leader is often a non-profit organization or a government-mandated institution (Provan & Kenis, 2007).

Figure 2. Basic forms of network management
(inspired by Provan & Kenis, 2007)



Concluding this theoretical part, it is important to recall the existence of a substantial difference between network governance and governance of networks. Network governance refers to the fact that governments develop (cyber-) security within a '*network*' and through horizontal coordination between bureaucratic organisations or agencies. However, network governance does not - by default - ensure a positive network level outcome or network effectiveness. For networks to be effective, they need to be internally governed or managed. The latter is referred to as the '*governance of networks*'-concept.

However, there remains a limited understanding amongst government managers on how to govern inter-agency networks as they approach networks from a rather traditional bureaucratic or hierarchical approach. A way to advance knowledge is by analysing the way governments design inter-agency networks, as network design influences the managerial aspects of cyber security networks. In doing so, it will also provide better insights on how to make cyber security networks more effective and efficient.

c. Cyber Security Governance in Belgium

While cyber security is nowadays considered as an essential part of Belgium's national security (FOD Kanselarij van de eerste minister, 2005; Centrum voor Cyber Security Belgium[CCB], 2015; FOD Defensie, 2014), the development of a national cyber security

authority – called the Cyber security Centre of Belgium (CCB) has not been self-evident as will be demonstrated in the following case-study.

The motivation for focussing on the national authority stems from the fact that this organisation has only recently been created. Hence, little or no research exists about the characteristics of this governance mechanism. The case-study aims to fill this knowledge gap by analysing the contextual factors which ultimately led to the creation of the CCB. The study develops around available governmental documents covering the period from the beginning of the millennium till the end of 2016. It is exactly in this timeframe that the consecutive governments - deliberately or not - shaped the current cyber security governance structure in Belgium.

d. In the aftermath of the 'Millennium bug' hysteria…

At the end of December 1999, while everybody was preparing to celebrate the arrival of the new millennium, cyber fear reigned in Belgium as in other parts of the world. It was envisaged that the beginning of the year 2000 would turn software into a common point of failure, resulting in a worldwide crash of embedded computer systems (Belga, 1999; Jones, 2014).

In retrospect, this global threat - commonly referred to as the '*Year 2000 problem*' (Y2K problem) or '*Millennium bug*' – represented a signal event as it marks the beginning of cyber security governance frameworks. Though the Y2K was primarily considered as a business issue, governments also- often supported by the UN or the World Bank - started to strengthen national coordination efforts in key sectors. For example, on New Year's Eve the Belgian government activated national or regional/provincial crisis centres with the objective to monitor the evolving overall national situation or take specific measures in dealing with possible disruptions (De Ruyck, 1999; Thomas, 2017).

Though New Year's Eve passed without major incidents being reported (Vermeulen, 2000), the Belgian Ministerial Committee for Intelligence and Security (Ministerieel Comité voor Inlichtingen en Veiligheid) decided in February 2000 to create a workgroup. The mission of this group was to explore whether the competences of a federal public agency could be extended towards the domain of encryption and protection of information. However, as the working group soon concluded that no such agency could be identified, the mandate of this group was redefined towards the potential creation of a new agency (Pieters, 2014).

Because of budgetary constraints, the idea of creating a new agency was abandoned in 2005. An alternative solution was found in the development of an informal consultation platform called '*the Belgian Network & Information Security*' (BelNIS). The objective of this platform was to collect knowledge and develop recommendations regarding information security (Belgische Senaat, 2012). It operated under the presidency of the minister in charge of digitalisation while the Federal Public Service for Information and Communication Technology (FEDICT) took up the '*network secretariat*' role (Belgische Senaat, 2012; Pieters, 2014).

Six years later - in 2011 - the government created the '*Computer Emergency Response Team*' (CERT) and implemented its policy statement concerning the development of a federal security policy on information networks and systems (Pieters, 2014).

In the second half of 2012, the government decided to install a working group to reflect on concrete proposals for the development of a national cyber security strategy

(Pieters, 2014).On 3 October 2012, it also presented its first '*Cyber Security Strategy*'. In addition, the Council of Ministers instructed the Prime Minister - on 21 December 2012 - to coordinate the execution of the cyber security strategy (Belgische Senaat, 2013).

Nearly a year later - on 6 November 2013 - the government announced its decision to speed up the execution of the cyber security strategy and to release the budgetary means for setting up a Centre for Cyber security in Belgium (FOD Kanselarij van de eerste minister, 2013).

Six months later - in 2014 - the government took a decision regarding the real allocation and destination of the in November 2013 reserved budget (Pieters, 2014). Later that year, the ultimate decision to set up the '*Cyber security Centre of Belgium*' (CCB) was taken (FOD Kanselarij van de eerste minister, 2014).The aim of the CCB was designed as to develop a centralised and integrated cyber security approach.

Finally, the CCB started its operational activities in January 2015 (CCB, 2015).

e. The Belgian inter-agency cyber security capability

The recent creation of the CCB is the final phase in the build-up to an integrated cyber security coordination in Belgium. However, based on theoretical insights, it is fair to claim that the mere fact that an inter-agency network is developed is in no way a guarantee or certitude that cyber security is or will be governed effectively or efficiently. Network effectiveness, as scholars argue, depends on two factors: network design and internal network governance. The analysis of the first issue - network design -is discussed in the next section, followed by the discussion on internal network governance aspects.

2. Network design

The analysis shows that the Belgian government had no intention to develop a 'networked' cyber security governance in 2002 (Pieters, 2014). Apparently, the government considered hierarchical forms of organisation to be the most effective approach to inter-agency coordination. The decision to create a workgroup with the task to assess the extension of the competences of a federal agency seems to confirm this view.

The decision to develop a '*networked*' cyber security governance followed in 2005.Budgetary constraints prevented the government from establishing a new agency. The only viable option was to set up an informal inter-agency platform called the '*Belgian Network & Information Security*' (BelNIS).

The members of the BelNIS platform are: the ministry responsible for the digitalisation of the State, the privacy commission, the national security authority (NVO), the social security, the postal and telecommunication service (BIPT), the federal computer crime unit from the federal police (FCCU), the military intelligence service (ADIV), the ministry of economy, the federal service for information and communication technology (FEDICT), the national crisis centre, the civil intelligence service (SVVE), the agency responsible for the science policy, the ministry of justice, the federal prosecution office, the college of prosecutors-general and the national agency responsible for coordination and threat analysis (OCAD) (Senaat, 2012).

The BelNIS network adapted a '*full-matrix*' or '*all-shared*' concept as the platform provided the opportunity for field experts from various governmental agencies to meet once a month and to discuss and consult each other about cyber related issues (Dallemagne, 2013; 2014).

In addition, it can be claimed that the 'BelNIS' platform acted as a '*goal-directed*' network organization as it consisted of more than three independent governmental organisations or agencies all working together to achieve- not only their own goals - but to achieve a collective goal: enhancing cooperation and exchange of information amongst governmental organisations in the domain of cyber security in Belgium.

The analysis also demonstrates that - following the arrival of the Cyber security Centre of Belgium - the network may develop and adapt its design. As the CCB will undoubtedly claim a central role in the coordination and communication of information, the network may move into a '*hub*' or '*star*' design.

Internal network governance

The analysis of the governmental documents clearly shows that the BelNIS network initially operated in a cyber security policy vacuum as it took some time before the Belgian government developed its first cyber strategy (Pieters, 2014).

In its first cyber security strategy, the Belgian government does not reveal a lot on how '*internal'* cyber security governance should be conceived apart from the following reference: '*…a mechanism to centrally steer the development of an integrated cyber security strategy'* (FOD Kanselarij van de eerste minister, 2012). The second cyber security strategy - the 2014 military cyber security strategy - is however a bit more detailed. In fact, it considers cyber security coordination in Belgium to exist on two levels: a vertical ('*policy*') and a horizontal ('*operational*') level. The lead agency at the policy or vertical level is the National Security Council (NSC), while operational cyber security activities are coordinated at the - horizontal level - by the CCB (FOD Kanselarij van de eerste minister, 2015; CCB, 2015).

Cyber security governance at the vertical level consists mainly of preparing cyber security policy work within various platforms under the authority of the '*coordination committee for intelligence and security*' (FOD Kanselarij van de eerste minister, 2015). One of these platforms is dedicated to the issue of '*cyber security*' for which the CCB has been designed as '*pilot*' agency (CCB, 2015). The aim of the '*Cyber Security platform'* is to establish a national cyber security policy through consultation with the public-sector. This platform has a sub-platform for developing a policy regarding the issue of '*cyber intelligence*' aimed at enhancing the situational awareness of cyber threats. The activities within this sub-platform are coordinated by the military intelligence service (CCB, 2015).Whilst the objective of each platform is purely strategic, each platform is free to design its composition according to the needs of its mission. In doing so, the platforms aim to develop not only a top-down but also a bottom-up approach (FOD Kanselarij van de eerste minister, 2015).

Coordination at the horizontal level was - until the creation of the CCB - dealt with by a '*self-governed network*' as there was no formal organ in the BelNIS network which drove the network actors from above. The governance responsibility was shared amongst the '*participants*' within the platform. However, the operational start of the Cyber security Centre of Belgium (CCB) may have serious consequences for the way governance is coordinated at the operational level. The CCB is now considered to be the national coordination body (FOD Defensie, 2014) ensuring the operational coordination of cyber security incidents (FOD Kanselarij van de eerste minister, 2012; Dallemagne, 2014). Governance is now '*brokered*' as the '*self-governed network'* seems to have moved towards a

'lead organisation' type of network with the core of the governance power located within a network actor.

However, concerns may be raised whether the coordination or management of information, resources, activities and competencies of the cyber security network is well organised as the analysis clearly demonstrates that none of the governmental documents – the Royal Decree concerning the development of the CCB - include clear references to '*network management*'. Based on this, it may be argued that network management has been developed rather '*haphazardly*' and does not stem from consciously planning and development.

In fact, though the 2012 '*Cyber Security Strategy*' suggested a centralization and integration of cyber security governance by a central body (Pieters, 2014), the government had no appetite to create a national cyber security authority. The 2013 and 2014 decisions - ultimately - leading to the creation of the Cyber security Centre of Belgium were taken due to external pressure. The first wave of pressure appeared in June 2013 when the hacking of Belgian's national telecom operator previously called '*Belgacom*' (nowadays known as '*Proximus*') was disclosed followed by revelations regarding the activities of '*allied*' or foreign intelligence services such as the American National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ). The second wave of external pressure surfaced when the hacking of the Ministry of Foreign Affairs was made public, a few weeks before the national elections of 2014 (Pieters, 2014).

As a way of conclusion, it can be argued that the creation of the Cyber security Centre of Belgium signifies without doubt a tremendous change in the way cyber security is governed in Belgium. It marks the beginning of a '*whole of government'* (Christensen & Laegreid, 2007) approach. While the CCB's main task is to provide an integrated and centralised coordination of cyber security(FOD Kanselarij van de eerste minister, 2014), it also represents a policy vision to move public sector organizations back from the disintegration of New Public Management (NPM)to more integration and coordination. With the arrival of the CCB, the Belgian government seems to make a statement that its intention is not 'to roll back' from the cyber security debate, but to become a '*coordinator*' and '*facilitator*'.

However - based on the analysis of the available governmental documents - it is fair to express Concerns about the effectiveness and efficiency of the '*internal governance*' at operational level, considering the rather '*haphazard*' way in which the CCB emerged. There are reasons to believe that the '*internal governance*' remains the result of an old-school top-down public management or '*government*' approach.

Conclusion and Recommendations

The threat of cyber is here to stay. Worse still, it is assumed that these cyber threats will become wicked as computer systems become more embedded and information and communication technologies make our society increasingly interdependent.

Cyber security is not only a technological or legislative complex issue as complexity also stems from the uncertainty on how to shape coordination and cooperation between governmental departments and agencies.

Whilst several governments started to develop formal and informal network forms of organisations to enhance the effectiveness and efficiency of cyber security governance, knowledge on how to manage and control the activities of the various network actors is

still lacking. This scarcity is rooted in the fact that criminologists remain mainly focussed on analysing dyadic relations between the constituting organizations of security networks, while various scholars stress that structural factors such as '*network design*' and '*network governance*' are decisive for the overall effectiveness and efficiency of networks.

To meet this concern this research was developed with the objective to analyse available governmental documents related to the development of a national cyber security authority in Belgium. The purpose was to identify whether the Belgian national cyber security authority was consciously planned and developed.

Aware of the fact that a single-case study is not sufficient to draw generalisations, the analysis nevertheless shows that the internal government of the Belgian cyber security network developed from an informal self-governed network into a Weberian '*hierarchical*' governed network. Though the analysis may not be supported by previous research, as little recognition has been given to the managerial aspects of networks by criminologists, it clearly demonstrates that cyber security governance in Belgium evolved rather accidentally. The creation of the current national cyber security authority seems to be the outcome of responding to '*external*' pressures rather than being the fruit of a consciously planned and executed government vision. Evidence for this claim is recovered from the fact that the government, initially, had the intention to govern cyber security in the old-school traditional governmental way by concentrating the responsibilities in an existing federal agency or even by developing a new agency. However, budgetary constraints ultimately forced the government to opt for an alternative. As a matter of fact, these financial issues led to the introduction of the network governance approach in the domain of cyber security in Belgium. The BelNIS platform represented an informal network initially having an '*all-shared*' design with internal governance being left over to the participants. This made BelNISto be considered as a '*self-governed*' network structure, more over as BelNIS operated in a policy vacuum as a national cyber strategy lacked. Even the arrival of the first cyber security strategies in Belgium did not automatically result in the Belgian government to consciously develop an integrated cyber security governance mechanism. Again, external pressures forced the Belgian government to haphazardly adapt its strategies and to develop the Cyber security Centre of Belgium. The latter is now considered to be the national cyber security authority. As such it can be argued that cyber security governance in Belgium is now developed through a '*hub*' network with governance by brokered by a '*lead organization'*.

In addition, the analysis also clearly demonstrates that '*internal*' network governance is not necessarily the result of an organic process as external pressures may force governments to impose or dramatically change the way networks are governed. The latter is clearly the case in Belgium. This may have far-reaching consequences on relationships between network actors, network policies, network technologies as well as the network culture.

The current case-study also emphasizes the necessity for cyber criminologists to focus on the managerial aspects of cyber security networks, besides technological or legislative aspects. Additional analysis of management aspects is required on how to develop and govern dedicated multi-organisational networks effectively and efficiently in a continuously growing complex or '*wicked*' cyber society.

Concluding this research, it is recommended to approach the issue of cyber security governance from a design-oriented research perspective as the latter may allow cyber criminologists to generate new insights. Design oriented research allows scholars to focus

on the perspective of professionals in a unique situation and who need to solve a field problem such as - in this case - managing a multi-organisational cyber security network. As such it aims to deliver science-based – generic – knowledge allowing to improve the actions of professionals in solving specific issues in organisations. The outcome of design-oriented research in the domain of cyber security, will without doubt serve the delivery of a more effective and efficient cyber security governance as it focuses on the design and development of proposals which professionals can apply to steer the organization in the desired direction.

References

Agranoff, R., & McGuire, M. (2007). Public Management Research Association Conference 2007. *Answering the big questions, asking the bigger questions: Expanding the public network management empirical reserach agenda.* Tuscon: Public Management Research Association.

Antivachis, N., & Angelis, V. (2015). Network Organizations: The Question of Governance. *Procedia - Social and Behavioral Sciences 175.*

Belga. (1999, December 14). *TV-nieuwsdienst volgt millennium (bug) op de voet.* Retrieved from Gazet van Antwerpen Nieuws: http://www.gva.be/cnt/oid73766/archief-tv-nieuwsdienst-volgt-millennium-bug-op-de-voet.

Belgische Senaat. (2012, juni 7). Senaat Schriftelijke vraag nr. 5-6424 van Alexander De Croo (Open Vld) aan de vice-eersteminister en minister van Binnenlandse Zaken en Gelijke Kansen. Brussel: Belgische Senaat.

Belgische Senaat. (2013, juli 5). Senaat Schriftelijke vraag nr. 5-9462 van Karl Vanlouwe (N-VA) aan de vice-eersteminister en minister van Binnenlandse Zaken en Gelijke Kansen. Brussel: Belgische Senaat.

Bisschop, L. (2012). *Governance of transnational environmental crime: Case study research on the illegal trade in e-waste and tropical timber.* Gent: Ghent University.

Bisschop, L., & Verhage, A. (2012). The complex(ity) of policing dirty crime. *Politie Studies & Currents of Policing, 25.*

Brewer, R. (2017). Controlling crime through networks. In P. Drahos, *Regulatory Theory: Foundations and Applications.* Canberra: ANU E Press.

Brodeur, J.-P., & Dupont, B. (2006). Knowledge Workers or "Knowledge" Workers? *Policing & Society, 16(1).*

Burris, S., Drahos, P., & Shearing, C. (2005). Nodal governance. *Australian Journal of Legal Philosophy, 30.*

Castells, M. (2000). Materials for an exploratory theory of the network society. *The Britisch Journal of Sociology, 51(1).*

Centrum voor Cyber Security Belgium. (2015). *Centrum voor Cyber Security Belgium. Jaarverslag 2015.* Brussel : Centre for Cyber security Belgium.

Charbonneau, M. (2012). New Public Management. In L. Côté, & J.-F. (. Savard, *Encyclopedic Dictionary of Public Administration, [online].* www.dictionnnaire.enap.ca.

Christensen, T., & Laegreid, P. (2007). The Whole-of-Government Approach to Public Sector Reform. *Public Administration Review.*

Clemente, D. (2011). International Security: Cyber Security as a Wicked Problem. *The World Today, Vol. 67, No 5, Issue 10*, 15. Retrieved from Chatham House. The Royal

Institute of International Affairs. : https://www.chathamhouse.org/publications/twt/archive/view/178579.

Commissie voor de Binnenlandse Zaken, de Algemene Zaken en het Openbaar Ambt. (2015). 05 Vraag van de heer Brecht Vermeulen aan de eerste minister over "de bescherming van de kritieke infrastructuur" (nr. 7616). Brussel: Commissie voor de Binnenlandse Zaken, de Algemene Zaken en het Openbaar Ambt.

Dallemagne, G. (2013, juni 27). Voorstel van resolutie waarbij de oprichting wordt gevraagd van een Centrum voor cyberbeveiliging in België. Brussel: Belgische Kamer van Volksvertegenwoordigers.

Dallemagne, G. (2014, september 16). Voorstel van resolutie over de aanscherping van de cyberveiligheid in België. Brussel: Belgische Kamer van Volksvertegenwoordigers.

De Ruyck, H. (1999, December 12). *Provinciale veiligheidscel vangt millennumbug op*. Retrieved from Gazet van Antwerpen Nieuws: http://www.gva.be/cnt/oid74256/archief-provinciale-veiligheidscel-vangt-millenniumbug-op

Décary-Hétu, D., & Dupont, B. (2012). The Social network of Hackers. *Global Crime, 13 (3)*.

dS De Standaard. (2014, May 10). Buitenlandse Zaken dient klacht in na hacking. *dS De Standaard*.

Dupont, B. (2004). Security in the Age of Networks. *Policing & Society, Vol. 14, Nr. 1*.

Dupont, B. (2006). Delivering security through networks: Surveying the relational landscape of security managers in an urban setting. *Crime, Law and Social Change, 45(3)*.

Dupont, B. (2016). La gouvernance polycentrique du cybercrime: les réseaux fragmentés de la coopération internationale. *Cultures & Conflits, 102*.

Easton, M. (2015). Het managen van innovatie door een netwerkende publieke politie. De triple-helix als vehikel. In P. Ponsaers, W. Bruggemn, M. Easton, & A. Lemaitrre, *De toekomstpolitie. Triggers voor een voldragen debat*. Antwerpen (BEL)/Apeldoorn (NL): Maklu.

Europol. (2017, November 16). *European Cybercrime Centre EC3*. Retrieved from Europol: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Federale Politie. (2016). Nationaal veiligheidsplan 2016-2019. *Samen naar de kern van de zaak*.Brussel (BE): Federale Politie.

Flemming, J., & Wood, J. (2006). *Fighting Crime Together: The Challenges of Policing & Security Networks*. Sydney: University of New South Wales Press.

FOD Binnenlandse Zaken. (2014, December 08). Bulletin nr : B003 - Schriftelijke vraag en antwoord nr. : 005 - Zittingsperiode : 54. *De inspanningen bij de federale politie inzake computercriminaliteit*. Brussel : De Belgische Kamer van Volksvertegenwoordigers.

FOD Binnenlandse Zaken. (2016, October 14). Bulletin nr : B091 - Schriftelijke vraag en antwoord nr : 1590 - Zittingsperiode : 54 Cyber security - Politiemaatregelen. *Cyber security - Politiemaatregelen*. Brussel : De Belgische Kamer van Volksvertegenwoordigers.

FOD Defensie. (2014). *Cyber Security Strategy for Defence*.Brussel : FOD Defensie.

FOD Justitie. (2016). Kadernota. *Kadernota Integrale Veiligheid*. Brussel (BE): FOD Justitie.

FOD Kanselarij van de eerste minister. (2012, October 03). Cyber Security Strategy. *Cyber Security Strategy. Erkennen van cyberdreiging. Verbeteren van veiligheid. Kunnen reageren op incidenten*. Brussel: De Kanselarij.

FOD Kanselarij van de eerste minister. (2013, November 06). Algemene Beleidsnota van de Federale Overheidsdienst Kanselarij van de eerste minister. Brussel: Belgische Kamer van Volksvertegenwoordigers.

FOD Kanselarij van de eerste minister. (2014, October 10). Koninklijk besluit tot oprichting van het Centrum voor Cyber security België. *Koninklijk besluit tot oprichting van het Centrum voor Cyber security België*. Brussel : Belgisch Staatsblad.

FOD Kanselarij van de eerste minister. (2014, October 10). Koninklijk besluit tot oprichting van het Centrum voor Cyber security België. *Koninklijk besluit tot oprichting van het Centrum voor Cyber security België*. Brussel (BE): Belgisch Staatsblad.

FOD Kanselarij van de eerste minister. (2015, January 28). Koninklijk besluit tot oprichting van de Nationale Veiligheidsraad. *Koninklijk besluit tot oprichting van de Nationale Veiligheidsraad*. Brussel: Belgisch Staatsblad.

FOD Kanselarij van de eerste minister. (2015, January 30). Koninklijk besluit tot oprichting van het Strategisch Comité en Coördinatiecomité voor inlichting en veiligheid. Brussel (BEL): Het Belgisch Staatsblad.

FPS Chancellery of the Prime Minister. (2017, April 27). *The Belgian Council of Ministers gives the green light to the very first National Cyber Emergency Response Plan*. Retrieved from Charles Michel. Prime Minister of Belgium.: http://premier.fgov.be/en/belgian-council-ministers-gives-green-light-very-first-national-cyber-emergency-response-plan.

Grabher, G., & Powell, W. (2004). Introduction. In G. Grabher, & W. Powell, *Networks*.Cheltenham, UK: Edward Elgar.

Hajer, M., Van Tatenhove, J., & Laurent, C. (2004). *Nieuwe vormen van Governance. Een essay over nieuwe vormen van bestuur met een empirische uitwerking naar de domeinen van voedselveiligheid en gebiedsgericht beleid*.Bilthoven (NL): RIVM.

Hojsgaard Munk, T. (2015). *Cyber-security in the European Region: Anticipatory Governance and Practices*. Manchester: University of Manchester.

Hood, C. (1991). A new public management for all seasons. *Public Administration, 69(1).*

Hunton, P. (2010). Cyber Crime and Security: A New Model of Law Enforcement Investigation. *Policing, Vol. 4, Nr. 4,*.

Jones, L. (2014, December 31). *How the UK coped with the millennium bug 15 years ago*. Retrieved from BBC news: http://www.bbc.com/news/magazine-30576670.

Kamarck, E. (2002). *Applying 21st-Century Government to the Challenge of Homeland Security*. Arlington, VA: The PricewaterhouseCoopers Endowment for The Business of Goverment.

Kapucu, N. (2014). Complexity, Governance, and Networks: Perspectives from Public Administration. In G. Morgöl, & G. Teisman, *Complexity, Governance & Networks*. Amsterdam: Baltzer Science Publishers.

Kerkhofs, J., & Van Linthout, P. (2013). *Cybercrime*. Uitgeverij Politeia NV.: Brussel (BEL).

Leukefeldt, R. (2016). *Cybercriminal networks. Origin, growth and criminal capabilities*. Den Haag (NL).

Leukefeldt, R., Veenstra, S., & Stol, W. (2013). *De strafrechtketen in een gedigitaliseerde samenleving. Een onderzoek naar de strafrechtelijke afhandeling van cybercrime.* De Bilt/Leeuwarden (NL): PAC/NHL.

Lu, Y., Luo, X., Polgar, M., & Cao, Y. (2010). Social Network Analysis of a Criminal Hacker Community. *Journal of Computer Information Systems, 51*(2).

Mazurczyk, W., Drobniak, S., & Moore, S. (2016). Towards a Systematic View on Cyber security Ecology. In B. Akhgar, & B. Brewster (eds.), *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities.* Cham: Springer.

Monge, P., & Contractor, N. (2003). *Theories of Communication Networks.* Oxford : Oxford University Press.

O'Toole, L. (1997). Treating Networks Seriously: Pratical and Research-Based Agendas in Public Administration. *Public Administration Review, 57(1).*

Pieters, P. (2014). Het NATIONAAL centrum voor Cybersecuity. Brengt de lang verwachte dirigent eindelijk symfonie? *Het Politiejournaal.*

Pollitt, C. (2003). Joined-up government: A survey. *Political Studies Review, 1 (1).*

Provan, K., & Kenis, P. (2009). Towards an exogenous theory of public network performance. *Public Administration, 87(3).*

Provan, K., & Kenis, P. (2005). Public Management Research Association Conference 2005. *Modes of Network Governance and Implications for Network Management and Effectiveness.* Los Angeles: Public Management Research Association.

Provan, K., & Kenis, P. (2007). Modes of Network Governance: Structure, Management and Effectiveness. *Journal of Public Administration Research and Theory, 18.*

Provan, K., & Milward, H. (2001). Do Networks Really Work? A Framework for Evaluating Public-Sector Organizational Networks. *Public Administration Review.*

Pugh, D., Hickson, D., Hinings, C., & Turner, C. (1969). The context of Organisation Structure. *Administrative Science Quarterly. 14*(1).

Raab, J., & Kenis, P. (2009). Heading Toward a Society of Networks. Empirical Developments and Theoretical Challenges. *Journal of Management Inquiry, 18, nr.3.*

Rhodes, R. (1996). *Understanding Governance.* Buckingham: Open University Press.

Rhodes, R. (2007). Understanding governance: Ten years on. *Organization Studies 28(8).*

Rittel, H., & Webber, M. (1973). Dilemmas in a general theory of planning. *Policy Sciences, 4.*

Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and Cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security. 4*(6).

Schuilenburg, M. (2015). *The Securitization of Society. Crime, Risk, and Social Order.* New York and London: New York University Press.

Senaat. (2012, June 18). Retrieved from Schriftelijke vraag nr. 5-6521 van Karl Vanlouwe (N-VA) d.d. 18 juni 2012 aan de staatssecretaris voor Ambtenarenzaken en Modernisering van de Openbare Diensten, toegevoegd aan de minister van Financiën en Duurzame Ontwikkeling, belast met Ambtenarenzaken: https://www.senate.be/www/?MIval=/Vragen/SchriftelijkeVraag&LEG=5&NR=6521&LANG=nl

Shearing, C., & Johnston, L. (2010). Nodal Wars and network Fallacies: A Genealogical Analysis of Global Insecurities. *Theoretical Criminology.*

Smith, F., & Ingram, G. (2017). Organising Cyber Security in Australia and beyond. *Australia Journal of International Affairs. 71*(6).

Stoker, G. (2002). Governance as theory: Five propositions. *International Social Science Journal, 50 (155).*

Thomas, M. (2017, April 04). *What Really Happened in Y2K?* Retrieved from Gresham College: https://www.gresham.ac.uk/lectures-and-events/what-really-happened-in-y2k.

Tropina, T., & Callanan, C. (2015). *Self- and Co-regulation in Cybercrime, Cyber security and National Security.* Cham: Springer.

Turrini, A., Cristofoli, D., Frosini, F., & Nasi, G. (2010). Networking literature about determinants of network effectiveness. *Public Administration, 88*(2), 528-550.

van Dijk, J., & Winters-van Beek, A. (2009). The Perspective of Network Government. The struggle between hierarchies, markets and networks as modes of governance in contemporary government. In A. Meijer, K. Boersman, & P. Wagenaar, *ICTs, Citizens & Governance: After the Hype!* Amsterdam: IOS Press.

Van Ryckeghem, D., Bruggeman, W., Easton, M., & Ponsaers, P. (2014). Een visie voor de politie in 2015: stuurgroep opteert voor netwerkende politie. *Cahiers Politiestudies.* 3(32).

Vermeulen, B. (2000, January 06). *Ik zou die computervirussen toch maar niet onderschatten.* Retrieved from Gazet van Antwerpen Nieuws: http://www.gva.be/cnt/oid76060/archief-ik-zou-die-computervirussen-toch-maar-niet-onderschatten

Whelan, C. (2011). Network Dynamics and Network Effectiveness: A Methodological Framework for Public Sector Networks in the Field of National Security. *The Australian Journal of Public Administration. 70*(3).

Whelan, C. (2012). *Networks and National Security. Dynamics, Effectiveness and Organisation.* Farnham (UK): Ashgate Publishing Limited.

Willen, A. (2015, July 15). *Complicated or complex - knowing the difference is important.* Retrieved from www.linkedin.com: https://www.linkedin.com/pulse/complicated-complex-knowing-difference-important-will-allen.

Wood, J., & Dupont, B. (2006). Introduction: Understanding the governance of security. In J. Wood, & B. Dupont, *Democracy, Society and the Governance of Security.* Cambridge: University Press.

Yar, M. (2011). From the 'governance of security' to 'governance failure': refening the criminological agenda. *Internet Journal of Criminology.*

Yip, M. (2016, 12 28). *Social Network Analysis as a tool to study organised cybercrime.* Retrieved from School of Engineering and Computer Science. University of Southampton.: users.ecs.soton.ac.uk/lac/dtc/posters/yip.pdf.

Zandee, D., Rood, J., & Meijnders, M. (2015). *The realationship between external and internal security.* Den Haag (NL): Nederlands Institute of International Relations Clingendael.