

Analysing Cyber Security Coordination in Belgium: Governing Cyber Security via Networks

E. Sumathi, A. Santha Kumari, Y. Meena

^{1,2,3}Faculty of Engineering
Department of Computer Engineering

Article Info

Received: 10-11-2025 Revised: 13-12-2025 Accepted: 23-12-2025 Published: 05-01-2026

Abstract

Uncertainty surrounds the establishment and development of cyber security networks, even as governments create both official and informal structures, or "networks," to foster cooperation between government organisations and departments. When we look at what's happened recently in cyber security in Belgium, we see the second point. Instead of building a cyber security network organization, the 2012 decision to establish the Belgian cyber security center seems to include shifting toward a hierarchical network coordination method reminiscent of Weberian theory. According to this piece, There is an increasing need for government entities to broaden horizontal coordination mechanisms in response to the complexity of cyber threats. As a result, there is a rising need for criminological studies of cyber security network management. Network management knowledge generation is essential because network management is both a determinant of the efficacy and efficiency of cyber security networks and an integral part of the governance of cyber security in networks as a whole.

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

Introduction

1. Research on the rise of networked methods for managing security and crime control, as well as the pluralisation of police forces, is of considerable interest to modern criminologists (Dupont, 2004; 2006, Flemming & Wood, 2006; Wood & Dupont, 2006). Although there is a lot of writing on networks, most people still use the term based on their gut feelings about what a network is and how it should act (Brewer, 2017). Because of their interest in studying the different ways in which information and resources

flow across networks, many of these scholars concentrate on the nature and patterns of the relationships between the different actors in the network (Yip, 2016; Décary-Héty & Dupont, 2012). For example, Leukfeldt (2016), Sabillon, Cano, Cavaller, & Serra (2016), Leukfeldt, Veenstra, & Stol (2013), Hunton (2010), and Lu, Luo (2010) all deal with this topic.

Cao and Polgar (2010). This leads to theorising on well-organised groups of people who assume that horizontal partnerships are necessary for co-production activities (Brodeur &

International Journal of Cyber Operations and Cyber Security Governance

Volume 1 Issue 1, 2026

Dupont, 2006; Dupont, 2006; Schuilenburg, 2015; Van Ryckeghem, Bruggeman, Easton, & Ponsaers, 2014).

It is unfortunate that few criminologists investigate the governance aspects of networks in order to understand how governance influences network results, despite the fact that many academics argue that "network design" and "network governance" are critical to networks' overall efficacy and efficiency (Whelan, 2012). Consequently, studying the network in its whole or as an integrated whole has received very little focus up until now (Whelan, 2012). This suggests that criminological research should shift its primary emphasis from networks as a tool for networked (cyber-)security governance to "management of networks" or "governance of networks" (Provan & Kenis, 2007). The ongoing discussion about how government entities may better prevent and fight cyber crime has also prompted the demand for further study in this area. The proliferation of cyberattacks and the growing embeddedness or interdependence of computer systems are both contributing to the complexity of cyber threats. As a result, there is a growing need to address cyber-risks on a global scale by creating new security policies, procedures, and recommendations (Hojsgaard Munk, 2015). As a result of ratification and signature of international accords like the 2001 Budapest "Convention on Cyber Crime," several nations have enacted new or revised criminal laws (Kerkhofs & Van Linthout, 2013). In

an effort to improve international collaboration and data sharing, certain groups banded together and established regional platforms, including "the European Cybercrime Center" (EC3) (Europol, 2017). Concerns over organisational changes stem from the fact that we still don't know which companies excel in cyber defence (Smith & Ingram, 2017). The author of this piece has two goals in mind when they set out to fill this information vacuum. The terms "network governance" and "governance of networks" are defined more precisely. Also included is the transition from a loosely knit multi-disciplinary cyber security network to a formalised networked coordinating mechanism with a more "Weberian" bent.

This approach is significant because, as Rittel and Webber (1973) put it, "wicked" cyber security challenges may be better and more efficiently tackled via the network paradigm, which necessitates humility. 'One size does not fit all' when it comes to the network notion. Antivachis and Angelis (2015) and Turrini, Cristofoli, Frosini, and Nasi (2010) both state that internal governance is crucial to the success of any network organization.

A literature analysis and case study form the basis of the study's qualitative research approach, which is used to accomplish these aims. Academic publications on the topics of "network governance" and "governance of networks" from disciplines as diverse as public administration, sociology, criminology, and politics make up the bulk of this literature survey. This

International Journal of Cyber Operations and Cyber Security Governance

Volume 1 Issue 1, 2026

case study explores the evolution of Belgium's inter-agency cyber security capabilities via an examination of publicly accessible government documents spanning the years 2000–2016. Analysed here are the following documents: resolutions submitted to the Belgium Chamber of Representatives pertaining to "cyber security," cyber security strategies, policy statements, the royal decree establishing the Cyber Security Center of Belgium (CCB or Centrum voor Cyber security België) on October 10, 2014, the interdepartmental brief titled "Kadernota Integrale Veiligheid 2016-2019," the National security plan 2016-2019, the Cyber Security Center of Belgium strategic plan 2015-2020, and the 2015 CCB annual report.

Do not think of the study as following a straight path. An continual selection-process of determining research topics and choosing sources characterises the preparation. A plethora of available sources are combed through, and many desktop research sessions are scheduled. Using the following keywords: cybercrime, cybersecurity, police, governance, security network, and network forms of organization, relevant publications are obtained. Search engines on different websites, such as Google Scholar and ResearchGate, have these terms entered.

Limiting the scope of this essay is important due to the vastness of the area of study controlling cyber security. The goal is not to evaluate the efficacy of Belgium's inter-agency

cyber security capabilities since efficacy may be affected by several variables, some of which are internal and others of which are external (Kenis & Provan, 2009). To clarify the ongoing uncertainty surrounding the oversight of government networks in the realm of cyber security, this research seeks to provide a more comprehensive look at the recent past of cyber security governance in Belgium.

The ultimate goal is to provide something useful for conversations about public sector networks that are dealing with collective action problems, like providing cyber security in situations where various government agencies, including intelligence, public prosecutors, and law enforcement, need to collaborate online. It could highlight the significance of comparing management contingencies with network characteristics, procedures, and results for both practitioners and policymakers. Last but not least, this study's findings could help with cyber security network architecture.

There are two sections to the article. After this brief overview, the first part delves into the theory of network governance and how networks are governed. The paper concludes with conclusions and suggestions, while the second section delves into the examination of the case-study.

2. Network Governance or Governance of Networks?

Here we provide the theoretical groundwork for the rest of the article and try to define "network governance" and "governance of

networks" a little more precisely. Despite the seeming similarities, there is a world of difference between these two points of view.

a. Network governance

The social complexity of modern society makes it exceedingly difficult, if not impossible, to find simple solutions to problems like poverty, climate change, and marine pollution. Since these problems are complicated and interdependent, there is no clear way to resolve them; in fact, solving one part of them always brings up new ones (Rittel & Webber, 1973). A comparable "wickedness" has emerged in both criminal activity and security measures with the advent of digital information and communication technology (Castells, 2000). This led to a rise in the need for new approaches to crime prevention and security management that might replace the tried-and-true ways of the past (Klijn,

This led to a discussion in 2012 about whether a more "decentred" (Bisschop & Verhage, 2012) or "polycentric" (Yar, 2011) form of coordination has superseded the traditional hierarchical state-led security provision. A number of public-private police partnerships or "security networks" have emerged as a result of this shift, which is also known as the change from "government" to "governance." (The year 2004 by DuPont) A new school of thought known as "New Public Management" or the "Governance model" has emerged as an alternative to the traditional, top-down style of public administration

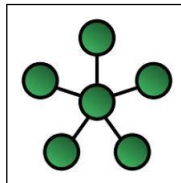
(Rhodes, 1996; Charbonneau, 2012; Pollitt, 2003; Stoker, 2002). Both the "New Public Management model" (Hood, 1991) and the "governance model" (Rhodes, 1996; 2007) attempt to optimise the public sector through inter-organizational, contractual relationships based on market principles, but the former is more focused on applying the network concept than on applying market principles (Klijn, 2012). According to this view of governance, "networks" or "network organisations" are a unique kind of social organization or structure that complements "markets and bureaucratic hierarchies" and may even lead to a number of benefits (Provan & Kenis, 2007; van Dijk & Winters-van Beek, 2009). More resources may be allocated to tackle "wicked" problems via networks, which are interconnected but autonomous structures of communication and trade. In a 2004 study, Hajer, Van Tatenhove, and Laurent

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). Another way to classify networks is as either "serendipitous" or "networks an sich" or "goal-directed" or "netzwerke für sich" (Provan & Kenis, 2007). The first group includes what are known as "emergent" or "informal"

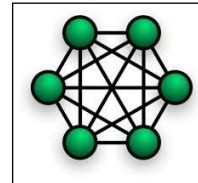
networks, which are formed in an unplanned and unstructured manner (Monge & Contractor, 2003). According to Walshan (2012), the second kind of network is known as a "goal-directed" network, and it consists of networks that are

intentionally designed and organised. The qualities and procedures of each design impact the information exchange and the 'internal' governance of the network in their own unique ways (Provan & Kenis, 2007).

Figure 1. Basic types of network designs



Hub or star network



All-channel or full-matrix network

Every node in a "hub" or "star" network is responsible for coordinating and communicating with the other nodes in the network. On the other hand, under the "full-matrix network" or "all-channel" model, all of the actors are interdependent.

b. The 'governance of networks' concept

3. Networks are rapidly replacing traditional systems of government as a means of multilaterally coordinating responses to wicked or complicated problems (van Dijk & Winters-van Beek, 2009). The assumption that an issue may be solved automatically or "an sich" when a group of individuals "network" and interact horizontally is a common motivation for creating networks, which are typically developed in reaction to external pressure (Provan & Kenis, 2009). However, the significance of individual businesses' performance pales in comparison to the result at the network level, so network governance denotes more than just the attainment of organisational objectives (O'Toole, 1997). Thus, "network outcomes" are fundamental to the network governance approach

(Whelan, 2012), with "network effectiveness" serving as the most crucial, since it denotes the successful completion of network-level tasks that would ordinarily be impossible for individuals within an organization to complete on their own (Provan & Kenis, 2007). But "Network Euphoria" (Provan & Kenis, 2009) might be the outcome of the second idea, which is problematic. It is often believed that networks are a panacea and always provide good results, however this was shown wrong during the 2005 Hurricane Katrina devastation in New Orleans (van Dijk & Winters-van Beek, 2009).

This means that networks must be overseen or controlled from inside. 'Governance of networks' or 'internal network governance' is a term that comes up in literature. It means that at least three organisations in a partnership or network work together to manage their information,

resources, activities, and competences so that they can achieve a common goal (Provan & Kenis, 2007). It is largely because very few government employees have a firm grasp on the fundamentals of security network management that there is a dearth of information on how to structure internal network governance in public sector networks (Kamark, 2002). Government managers have a background and education in running more conventional bureaucracies, which they use to oversee networks. If you want your network members to take collective, mutually beneficial action and handle or resolve issues, you need to know how to manage networks. On top of that, it's about getting your hands on resources, whether that's via acquisition or control, and making sure they're being used well.

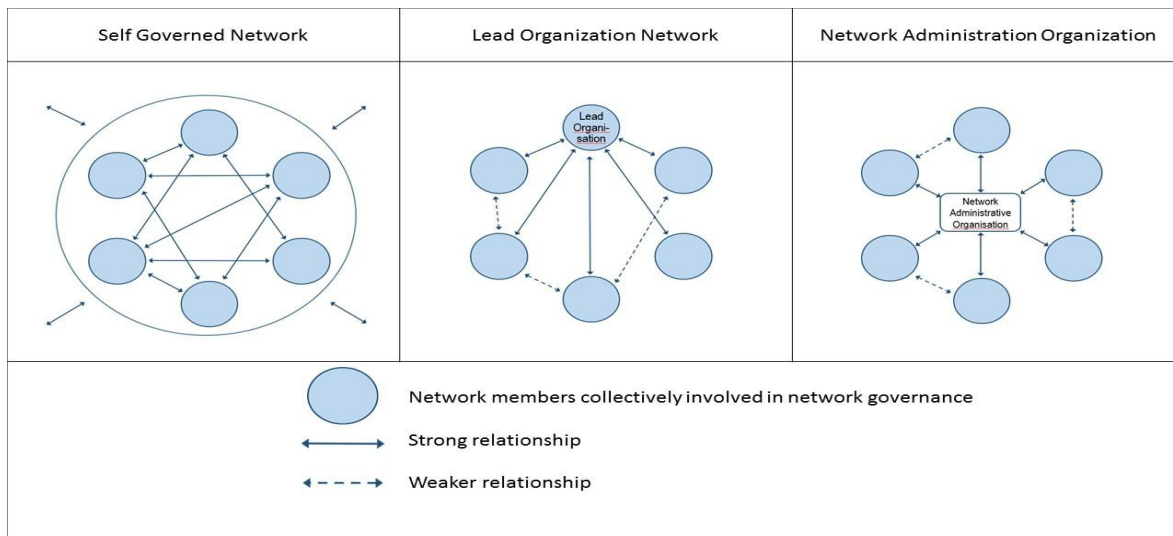
This leads us to the fact that there are two ways to classify internal network governance: all-shared and broken (Provan & Kenis, 2007).

The "participant governance" or "self-governed network" is the subject of the first category of governance (Provan & Kenis, 2007). Within this category, there isn't a hierarchical

structure that directs the players. Each partner is responsible for something, yet one person may take on more than one role. Accordingly, the actors' involvement is crucial to the framework (Agranoff & McGuire, 2007; Provan & Kenis, 2007). "Lead organization-governed networks" make up the second category of internal network governance. The governing structure of these networks is more centralised, with one core

Anybody participating in the system assumes command. The main actor usually rises to the top due to its access to or contribution to other types of "capital," such as financial, political, or symbolic assets (Dupont, 2004; 2006). According to Agranoff and McGuire (2007) and Provan and Kenis (2007), the role of the leading organization is to make it easier for the other players to carry out their tasks. The central authority for network governance under a "network administrative organization" model does not reside within the network itself but rather in an external entity. According to Provan and Kenis (2007), the external leader is often a government-mandated institution or a non-profit organization.

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



4. A major distinction between network governance and governance of networks must be kept in mind in order to conclude this theoretical section. The term "network governance" describes the way in which governments design and implement (cyber-)security measures via horizontal cooperation across many bureaucratic entities. Having said that, good network-level outcomes and efficacy are not guarantyd by default by network governance. Internal governance or management is essential for networks to function effectively. The second one is called the "governance of networks" idea. Although government managers approach networks from a more typical bureaucratic or hierarchical perspective, they still lack a thorough knowledge of how to control inter-agency networks. Since network design affects the management

components of cyber security networks, studying how governments construct inter-agency networks is a good method to enhance understanding in this area. Better understanding on how to improve the efficacy and efficiency of cyber security networks will also be gained from this.

a. Belgium's Cyber Security Governance

As this case study will show, it was not obvious that Belgium needed a national cyber security authority, the Cyber Security Center of Belgium (CCB), even though cyber security is now essential to the country's defence (FOD Kanselarij van de eerste minister, 2005; Centrum voor Cyber Security Belgium [CCB], 2015; FOD Defensie, 2014). Due to the organization's relative youth, there is an incentive to zero in on the national authority. As a result, the features of this governance system

have been the subject of little study. This case study intends to address that information vacuum by investigating the background circumstances that gave rise to the CCB. Using publicly accessible government papers spanning the years 2000–2016, the research takes shape. During this period, the present framework for cyber security governance in Belgium was established by the successive administrations, whether intentionally or not.

b. Ever since the "Millennium bug" panic...

Cybersecurity was a major concern in Belgium and throughout the globe in the latter days of 1999, just as everyone was getting ready to welcome the new millennium. It was thought that software would become a common weak spot at the turn of the millennium, leading to a global failure of embedded computer systems (Belga, 1999; Jones, 2014). This worldwide security risk, also called the "Millennium bug" or the "Year 2000 problem," was a watershed moment since it ushered in new regulations for online protection. Despite the fact that the Y2K was mostly seen as a commercial problem, countries, sometimes with the help of the UN or the World Bank, began to step up their national coordinating efforts in critical areas. For instance, in order to keep tabs on the changing national situation or cope with any potential disturbances, the Belgian government activated national or regional/provincial crisis centers on New Year's Eve (De Ruyck, 1999; Thomas, 2017).

A workgroup was established in February 2000 by the Belgian

Ministerial Committee for Intelligence and Security (Ministerieel Comité voor Inlichtingen en Veiligheid), despite the fact that no significant occurrences were recorded on New Year's Eve (Vermeulen, 2000). The group's stated goal was to determine whether a federal public agency's purview might be expanded to include data encryption and security. But as the working group quickly realised that no such agency could be found, its mission was refocused on the possibility of establishing a new agency (Pieters, 2014). Budgetary concerns led to the 2005 cancellation of plans to establish a new agency. A different approach was used by creating a venue for informal conversation known as "the Belgian Network G Information Security" (BelNIS). Information security was the focus of this platform's knowledge collection and recommendation development efforts (Belgische Senaat, 2012). The minister responsible for digitisation served as its president, and the Federal Public Service for Information and Communication Technology (FEDICT) assumed the position of "network secretariat" (Belgische Senaat, 2012; Pieters, 2014).

After waiting six years, in 2011, the government established the "Computer Emergency Response Team" (CERT) and put its policy statement into action for the creation of a federal strategy for the security of information networks and systems (Pieters, 2014). A working group was established in the latter part of 2012 by the government to consider specific

suggestions for the creation of a national cyber security policy.

Pieters (2014) states that...Meanwhile, its first "Cyber Security Strategy" was unveiled on October 3, 2012. The Prime Minister was also directed by the Council of Ministers on December 21, 2012. - to help put the cyber security plan into action in a coordinated manner (Belgische Senaat, 2013). After almost a year had passed, on November 6, 2013, the Belgian government declared that it would speed up the implementation of its cyber security policy and provide funds to establish a Center for Cyber Security (FOD Kanselarij van de eerste minister, 2013). The government finally decided in 2014, six months after the reserved budget was set aside in November 2013, where the money would really go (Pieters, 2014). According to the FOD Kanselarij van de eerste minister (2014), the final decision to establish the "Cyber Security Center of Belgium" (CCB) was made later that year. The objective of creating the CCB was to have a unified strategy for cyber defence. In January 2015, the CCB finally began operating (CCB, 2015).

a. The Belgian inter-agency cyber security capability

A comprehensive cyber security coordination framework has been developed in Belgium, with the establishment of the CCB being the last stage in this process. On the other hand, theoretical considerations suggest that the establishment of an inter-agency network does not ensure

efficient or effective governance of cyberspace.

Scholars contend that two aspects—network architecture and internal network governance—determine the efficacy of a network. Next, we'll go over some of the internals of network governance once we finish analysing the first problem, which is network architecture.

5. Network design

A 'networked' cyber security governance was not an objective of the Belgian government in 2002, according to the research (Pieters, 2014). It would seem that the government thought that the best way to coordinate amongst agencies was via hierarchical types of organization. This appears to be supported by the decision to establish a task force whose responsibility it is to evaluate the expansion of a federal agency's competencies.

The next year, in 2005, the decision was made to establish a "networked" cyber security governance system. The establishment of a new agency was impeded by budgetary restrictions. The only practical choice was to establish the "Belgian Network G Information Security," an informal venue for inter-agency collaboration. A number of government agencies and departments make up BelNIS, including: the ministry in charge of digitalisation, the privacy commission, the national security authority, social security, postal and telecommunication service, federal computer crime unit, military intelligence service, ministry of economy, federal service for information and communication

technology, national crisis center, civil intelligence service, ministry of justice, federal prosecution office, college of prosecutors-general, and national agency responsible for coordination and threat analysis (OCAD) (Senaat, 2012). Because it allowed for monthly meetings where specialists from different government departments could convene and talk shop about cyber challenges, the BelNIS network adopted a "full-matrix" or "all-shared" paradigm (Dallemagne, 2013; 2014).

It is also possible to argue that the 'BelNIS' platform was a 'goal-directed' network organization because it brought together more than three separate government agencies in Belgium that were all striving to improve cyber security through increased collaboration and sharing of information.

The investigation also shows that the network may evolve and change its layout when the Cyber Security Center of Belgium arrives. The network may adopt a "hub" or "star" layout due to the CCB's anticipated pivotal role in data coordination and transmission.

Internal network governance

Because the Belgian government did not establish its first cyber strategy for some time, the examination of official documents demonstrates that the BelNIS network functioned initially in the absence of cyber security policies (Pieters, 2014). The Belgian government's initial cyber security strategy provides few details regarding the ideal structure of "internal" cyber security governance, with the only

reference being to "...a mechanism to centrally steer the development of an integrated cyber security strategy" (FOD Kanselarij van de eerste minister, 2012). On the other hand, the military's cyber security policy from 2014 provides a little more information. It goes so far as to say that there are two tiers of cyber security coordination in Belgium, one at the policy level and one at the operational level. According to the FOD Kanselarij van de eerste minister (2015) and the CCB (2015), the National Security Council (NSC) is the top agency at the policy or vertical level, while the Cyber Command and Control Board (CCB) is in charge of operational cyber security actions at the horizontal level.

The "coordination committee for intelligence and security" (FOD Kanselarij van de eerste minister, 2015) is responsible for overseeing cyber security policy work across several platforms at the vertical level of governance. The CCB serves as a "pilot" agency for a platform that focuses on "cyber security" (CCB, 2015). Through public-sector engagement, the "Cyber Security platform" aims to formulate a national strategy for cyber defence. The development of a policy on the topic of "cyber intelligence" to improve situational awareness of cyber dangers is a sub-platform of this platform. The military intelligence agency coordinates the actions within this sub-platform (CCB, 2015). Although all platforms have a strategic goal in mind, they are all allowed to shape their composition as they see fit in order to achieve that goal. According to the FOD Kanselarij van de eerste minister (2015), the platforms are striving to establish both a top-down and a bottom-up approach.

Since the BelNIS network lacked a formal entity to command its participants from on high, horizontal coordination was handled by a "self-governed network" prior to the establishment of the CCB. Everyone who was considered a "participant" on the platform was equally responsible for governance. The launch of the Cyber Security Center of Belgium (CCB) might, however, significantly alter the operational level of governance coordination. According to recent reports, the CCB is currently seen as the national coordination organization responsible for coordinating the response to cyber security events (FOD Defensie, 2014; FOD Kanselarij van de eerste minister, 2012; Dallemagne, 2014). With the "self-governed network" seemingly heading in the direction of a sort of network known as a "lead organization," where a network player serves as the central authority for governance. It is worth noting that the analysis shows that none of the government documents, including the Royal Decree regarding the development of the CCB, make explicit mention of "network management." This raises questions about the organization and coordination of the cyber security network's information, resources, activities, and competencies. This lends credence to the claim that network management is the result of ad hoc rather than deliberate design and development. Despite recommendations to establish a national cyber security authority in the 2012 "Cyber Security Strategy" (Pieters, 2014), the federal government showed little interest in carrying them out. Final judgements in 2013 and 2014 decisions that, in the end, resulted in the establishment of the Cyber Security

Center of Belgium were made in response to pressure from outside sources. In June 2013, the hacking of Belgium's national telecom operator, formerly known as "Belgacom" but now known as "Proximus," came to light, igniting the first wave of pressure. Subsequent revelations about the activities of "allied" or foreign intelligence services, including the NSA and GCHQ, further intensified the situation. Public revelations about the 2014 national elections' hacking of the Ministry of Foreign Affairs ushered in a second round of outside pressure (Pieters, 2014). In conclusion, it might be said that the establishment of the Cyber Security Center of Belgium unquestionably represents a massive shift in the regulation of cyberspace in Belgium. It is the first step toward a "whole of government" strategy (Christensen & Laegreid, 2007). In addition to its primary function of coordinating cyber defences (FOD Kanselarij van de eerste minister, 2014), the CCB embodies a policy goal of reversing the trend of disintegration that has befallen public sector organisations since the advent of New Public Management (NPM) and bringing them back together. Rather than "rolling back" from the cyber security discussion, the Belgian government seems to be aiming to become a "coordinator" and "facilitator" with the CCB's entrance. On the other hand, given the CCB's rather "haphazard" origins, it is reasonable to question the efficacy and efficiency of the "internal governance" at the operational level, according to the reviewed government papers. Some see the so-called "internal governance" as a holdover from the days of authoritarian

public administration.

Conclusion and Recommendations

The cyber menace will persist. To make matters worse, our society is becoming more interconnected due to the proliferation of information and communication technology, which means that cyber risks are only going to become worse as computer systems get more ingrained.

The lack of clarity about how to influence collaboration and coordination between government departments and agencies adds another layer of complexity to the already formidable technical and legal challenges posed by cyber security.

There is a dearth of understanding on how to regulate and control the actions of the different network players, even if several governments have begun to establish official and informal network forms of organisations to improve the efficacy and efficiency of cyber security governance. The reason behind this dearth is that most scholars agree that structural factors like "network design" and "network governance" determine how efficient and effective a network is as a whole, but criminologists are still primarily concerned with studying the relationships between the organisations that make up security networks. In response to this worry, this study set out to examine official Belgian papers concerning the establishment of a national cyber security body. This investigation set out to determine if the Belgian national cyber security authority was deliberately designed and constructed.

Although this research does not aim to generalise, it does demonstrate that the

Belgian cyber security network's internal governance evolved from a decentralised, self-governed structure to a more formal, hierarchical one, following the paradigm of Weberian networks. Although the findings may not be supported by prior studies, as criminologists have paid less attention to the administrative parts of networks, the study does show that cyber security governance in Belgium developed more by chance. Instead of being the product of a well-thought-out government strategy, the establishment of the present national cyber security body seems to have been a reaction to "external" demands. The fact that centralising the duties in an existing federal agency or even creating a new one was the original plan to manage cyber security in the conventional sense lends credence to this assertion. But in the end, the government had to choose an alternative due to fiscal concerns. Actually, the implementation of the network governance strategy in the field of cyber security in Belgium was prompted by these financial concerns. At its inception, the BelNIS platform stood for a loosely knit network whose members were initially responsible for deciding how to run the show internally. Additionally, as there was no national cyber strategy in place, BelNIS functioned in a policy vacuum, earning it the label of a "self-governed" network structure. Despite the introduction of first cyber security initiatives, the Belgian government did not immediately set out to create an integrated framework for cyber security administration. Once again, the Belgian government was compelled to build the Cyber Security Center of Belgium due to external constraints, which caused haphazard strategy adaptations. The

latter is now thought of as the head of the country's cyber defences. One may say that a "lead organization" is currently mediating the development of cyber security governance in Belgium via a "hub" network. Furthermore, the research shows that governments may be compelled to impose or drastically alter network regulation due to external forces, thereby proving that "internal" network governance is not static. In Belgium, the second scenario is obviously true. This may significantly alter the dynamics of the network and its culture, as well as its policies, technology, and actors.

This case study also shows how important it is for cyber criminologists to pay attention to the legislative and managerial parts of cyber security networks. In a cyber society that is always evolving into something complicated, or "wicked," more research into managerial factors is needed to determine the best way to build and oversee specialised multi-organizational networks.

In conclusion, cyber criminologists may benefit from adopting a design-oriented research stance when tackling the problem of cyber security governance. This stance has the potential to provide fresh insights. Researchers may put themselves in the shoes of working professionals by doing design-oriented research. In this example, they are trying to figure out how to manage a cyber security network that connects many organisations. Therefore, it seeks to provide science-based, general information that may enhance professionals' activities in addressing organization-specific problems. A more effective and efficient cyber security

governance will undoubtedly be the end result of design-oriented research in the cyber security domain. This type of research focuses on creating proposals that professionals can use to guide the organization in the right direction.

References

With McGuire, M. (2007) as the author. Meeting of the Public Management Research Association in 2007. Enhancing the agenda for public network management empirical research: addressing the major issues while posing the larger ones. Arizona: Association for Public Management Research, Tuscon. In 2015, Antivachis and Angelis published a paper. Organisational Governance in Networks. Article 175. In the field of social and behavioural sciences. (December 14, 1999) in Belga. The TV news service is following the millennium bug closely. According to the Belgian Senate, as cited in Gazet van Antwerpen Nieuws (2012, juni 7), the chief newsreader of television station TVN "Volgt" the millennium bug on the air. Printed question no. 5-6424 from Alexander De Croo (Open Vld) to the vice-prime minister and minister of Foreign Affairs and Foreign Trade. Belgium Senate, Brussels.

The Belgian Senate. (Juli 5, 2013). Senate written question no. 5-9462 from Karl Vanlouwe (N-VA) to the vice-prime minister and minister of Foreign Affairs and Foreign Affairs. Belgium Senate, Brussels. The author of the article is Bisschop (2012). Research on the illicit trafficking in tropical wood and electronic trash as a case

International Journal of Cyber Operations and Cyber Security Governance

Volume 1 Issue 1, 2026

study of transnational environmental crime governance. University of Ghent in Gent. Published in 2012 by Bisschop and Verhage. The intricacy of combating corrupt law enforcement. Brewer, R. (2017) stated in *Politie Studies G* Currents of Policing, 25. Manage criminal activity via interconnected systems. Foundations and Applications of Regulatory Theory, edited by P. Drahos. New South Wales: Australian National University Press, Canberra. B. Dupont and J.-P. Brodeur (2006). Workers with Knowledge or Workers with "Knowledge"? Society for Policing Quality, 16(1). Published in 2005 by Burris, Drahos, and Shearing. Administration at the node level. The Australian Journal of Legal Philosophy, Issue 30, 30. It was written by Castells in the year 2000. Theoretical foundations for a network society inquiry. Published in volume 51, issue 1, of the British Journal of Sociology. Cyber Security Center Belgium. 2015 was the year. Cyber Security Center Belgium. Final report 2015. Cybersecurity Center of Belgium, Brussels. The year 2012 was written by Charbonneau. Modern Public Administration. Available online at www.dictionnaire.enap.ca, this entry is from the Encyclopedic Dictionary of Public Administration, edited by L. Côté and J.-F. Savard. P. Laegreid and T. Christensen (2007). A Government-Wide Strategy for Reforming the Public Sector. The Journal of

Public Administration. In 2011, Clemente published a work. Concerns about cyberspace and international stability: a tough problem. Chapter 67, Issue 5 of *The World Today*, pages 10–15. Acquired from the Chatham House database. The Viceroy