Cyber Intelligence Networks: A Typology

Jori Pascal Kalkman and Lotte Wieskamp

ABSTRACT
In this research, we identify different types of cyber intelligence networks and specify their unique characteristics. While existing research discusses intelligence cooperation in general terms or analyzes single case studies, we provide insight in the diversity of cyber intelligence networks in existence. Based on a qualitative study of cyber intelligence networks in the Netherlands, we identify four distinct types: centralized networks, business networks, operational networks, and local networks. These networks differ in terms of their history, activities, governance structure, communication frequency, goal consensus, member commitment, and perceived results. Based on the typology, we claim that the network type influences the challenges and outcomes of cyber intelligence cooperation. Next, we argue for an expanded focus on private sector engagement in these networks. Lastly, we advocate for incentivizing bottom-up cyber intelligence cooperation.

ARTICLE HISTORY
Received 27 July 2018
Revised: 4 December 2018
Accepted 9 February 2019

KEYWORDS
Cyber; intelligence; networks; typology; cooperation

Introduction
Cyber security increasingly demands inter-organizational cooperation due to the rise of new, diverse, and transnational cyber threats (Cozine, 2016; Mattern, Felker, Borum, & Bamford, 2014; Rudner, 2013). Such threats can be of various natures. For instance, cyber-terrorism can be used to create fear of violence for political purposes and as a means to gather support for violent groups (Trim, 2003), while cyber-attacks can be launched with state support to sabotage or spy on other entities (Claver, 2018; Tikk, 2011). Next, malicious criminals and activists may hack into computer systems of companies and governments to disrupt their functioning or steal valuable assets (Stouder & Gallagher, 2013; Trim, 2003). Lastly, there is a risk of insider threat, emanating from dissatisfied staff members sabotaging or protesting against their own organization in this manner (Rudner, 2013). Staff members’ unawareness or negligence may further exacerbate these threats.

Cyber intelligence on the capabilities and plans of malicious actors is needed to anticipate and protect against cyber threats (Jasper, 2017;
Following Gill and Phythian (2006, p. 19), we define intelligence as ‘a process of gathering and analyzing information with a view to providing forewarning and shaping policy so as to protect or enhance relative advantage’. In the context of cyber security, this means that ‘capabilities, intentions, and activities of potential adversaries and competitors, as they evolve, in the cyber realm’ need to be understood and analyzed (see Mattern et al., 2014, p. 704). With cyber intelligence, public and private organizations can strengthen their cyber security and protect digital privacy, property, and critical infrastructures (Carr, 2016).

The complexity and speed of current cyber threats renders it virtually impossible for organizations to manage them independently. Instead, as isolated action will be unable to keep up with fast-developing cyber threats, there is an ‘urgency to build a shared intelligence’, for which ‘cooperation and openness are key’ (Velasco, 2017, p. 1). Such cooperation is most effective when it extends over boundaries to include not only traditional public security providers but also private actors (see Carr, 2016; Vogel et al., 2017). Although the need for an active role of both public and private parties in cyber security networks is uncontested, cyber collaboration often proves problematic in practice. Yet, while there is considerable research on international and national partnerships among public intelligence organizations, little is known about the collaboration with and among private parties in cyber intelligence networks (or cyber security networks).

In this exploratory study, we dive into the question of cyber intelligence cooperation between the broad range of cyber intelligence actors, which in this research refers to any public or private organization collecting, analyzing, or using cyber-related intelligence. In line with the interests of contemporary intelligence studies, we take a network perspective on the cyber intelligence domain and specifically address questions regarding the characteristics and functioning of cyber intelligence networks (see Gill & Phythian, 2016). A network focus enables us to describe the various, complex relations between organizational actors, as it is ‘the most general category of coordination’ (Gill & Phythian, 2006, p. 40). We use this perspective to study cyber intelligence networks in the Netherlands. This exploratory study informs the answer to our research question: What types of cyber intelligence networks can be distinguished and what are their characteristics?

Based on our data, we identify four ideal-typical cyber intelligence networks with unique histories, network elements, and results. We find that these cyber intelligence networks differ to such an extent that it is necessary to attend more closely to the diversity of cyber intelligence networks in discussing the challenges and outcomes of intelligence collaboration. Additionally, we argue for more attention for private sector involvement in cyber intelligence networks and we advocate for incentivizing bottom-up initiatives for cyber intelligence collaboration.
This paper proceeds with discussing the reasons for intelligence cooperation and briefly reviews literature on intelligence collaboration in the public sector. Subsequently, we discuss insights on public-private cyber security partnerships and networks. This leads us to conclude that a systematic analysis and comparison of the broad range of cyber intelligence networks is still absent. After we have introduced our case and methods, we therefore present four types of cyber security networks and discuss their characteristics. In the discussion and conclusion, we reflect on the theoretical and practical limitations and implications of our study.

Theory

The need for cyber intelligence cooperation

Given the new and rising cyber security threats (Rudner, 2013), there is widely accepted consensus that no intelligence actor can successfully act alone (see Lefebvre, 2003; Parkes, 2017). Instead, effective cyber security management requires the collective effort of various actors (see Pascovich, 2017). On the international level, intelligence agencies of various countries have banded together in partnerships and coalitions to share analyzed information quickly and efficiently (see Clough, 2004). Nationally, public intelligence agencies are mandated to work together (Lasoen, 2017), while private parties are increasingly encouraged to take the path of cyber intelligence sharing and collective cyber security actions as well (see Harknett & Stever, 2009; Shore, 2015; Tikk, 2011). If such efforts fail, ‘there is a danger of intelligence not getting into the hands of the people who need it when they need it’ (Cozine, 2016, p. 195). This is why cyber intelligence operations require proactivity, an accurate and up-to-date threat environment understanding, and data-based decision-making (Mattern et al., 2014).

Recognizing the potential setbacks and risks of inactivity, an increasingly broad range of actors is getting involved in cyber intelligence, which enabled the emergence of cyber intelligence networks (Gill & Phythian, 2006). Unsurprisingly, these networks face certain collaboration problems and challenges. For researchers, this means there is a need for focusing on the ‘social and political’ side of intelligence gathering and usage, rather than a mere technical approach (Gill & Phythian, 2016, p. 8). Here, we first introduce insights of studies on public sector cyber intelligence cooperation. Afterwards, we discuss how private actor engagement is often introduced as elementary (or even a panacea), but we conclude that there is yet little comparative analysis between the different types of cyber intelligence networks in existence.
Public sector cyber intelligence cooperation

International intelligence collaboration, such as on issues of cyber security, often takes place between allied countries or under the flag of an international organization, such as NATO (Clough, 2004). Although being perceived as essential to safeguarding countries, in particular since 9/11 and with the rise of cyber threats, these collaborations are not without problems. In international forums, for instance, countries can simply distrust each other’s use of certain intelligence and therefore be hesitant to share it (Seagle, 2015). Bilateral agreements are consequently the more appealing alternatives. Even when trust between two (or more) intelligence agencies is present, however, other concerns may arise (see Lefebvre, 2003). Agencies may identify different threats and thus have a different focus, there may be legal hurdles, and intelligence can be used in unintended ways or be compromised in the process of cooperation (Lefebvre, 2003). The problematic intelligence collaboration between the US and Pakistan in the context of the war in Afghanistan serves as an example in this regard (Vestermark, 2017). Irrespective of these inhibiting factors, intelligence collaboration takes place internationally. Interestingly, this cooperation usually takes an informal shape and may be incidental rather than structural (Manjikian, 2015).

One would expect stronger intelligence collaboration on the national level, as there is political support for cyber intelligence sharing among public agencies. Yet, this optimism often proves unfounded. Intelligence collection and analysis appears to be very fragmented in many countries, as agencies operate in relative isolation, resulting in considerable barriers that problematize fruitful collaboration, as multiple case studies have demonstrated (see Cozine, 2016; James, Phythian, Wadie, & Richards, 2017; Parkes, 2017). This fragmentation results in the use of incongruent intelligence gathering processes and bureaucratic procedures that are not aligned (Cozine, 2016). In turn, as an analysis of the Belgian intelligence services shows, this fragmentation may reduce the motivation to cooperate among various actors or even simply prevent them from seeing the benefits (Lasoen, 2017). More problematically even, given that numerous intelligence agencies have similar or overlapping mandates, they may compete in turf wars (see Gill & Phythian, 2016). Turf wars are indeed a common problem as public agencies have their own interests and see other actors (within the government) as threats to their interests (Allison, 1971; Kalkman, Kerstholt, & Roelofs, 2018; Maekins, 2018). The resulting polarization may prevent operational synergy by instead creating stove-pipes, silence, and redundancy (Lasoen, 2017). In fact, ‘bureaucratic turf battles often act as a barrier to the necessary geographic and functional integration’ (Sloan, 2006, p. 203). Even though such considerations may seem petty, polarization appears to be persistent and is therefore not easily replaced with collaboration in practice. These experiences of
Public-sector cyber intelligence collaboration indicate at the need for reserved expectations of public-private collaboration on cyber security.

Public-private cyber cooperation

Recently, private sector engagement in cyber intelligence collaboration has gained considerable attention. Private involvement in the collective effort to improve cyber threat management has been widely recommended (see Carr, 2016; Stouder & Gallagher, 2013). Several North American authors even claimed that, ultimately, cyber security demands cooperation between public and private sector parties (Harknett & Stever, 2009; Shore, 2015). It is therefore not surprising that several governments have sought to establish public-private (or cross-sectoral) partnerships and networks for cyber intelligence sharing (see Gill & Phythian, 2006). In Canada, for instance, public-private networks have been set up to improve the sharing of collected and analyzed cyber information (Shore, 2015). Similarly, the UK’s National Infrastructure Security Co-ordination Centre brings together various parties to protect critical infrastructures against cyber threats (Trim, 2003).

In fact, there are multiple reasons for public-private collaboration in cyber intelligence. Primarily, these have to do with the nature of the cyber realm (or cyberspace). Cyberspace refers to the ‘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’ (US DoD, 2016, p. 58). Cyberspace, specifically, has three layers: a physical layer, existing of boxes and wires; a syntactic layer containing instructions of designers and users; and a semantic layer, consisting of the information in the machine (Libicki, 2009, p. 12–13). Public and private actors increasingly operate in cyberspace and consequently grow more and more interdependent. Exemplary, private companies may provide the necessary electronic hardware or internet access to public organizations, which in turn regulate cyber companies and private sector activities in the cyber realm. Due to their interdependence, public-private collaboration is needed in times of cyber threats. This collaboration is further encouraged by the changing nature of these cyber threats. In fact, current threats cannot be tackled by parties independently (Tikk, 2011). As cyber threats now pose one of the core threats to countries, governments are obliged to upgrade their cyber security management for which private support is essential (see Shore, 2015). By extension, the distinction between public and private responsibilities are growing ambiguous. For example, some of the threats to companies may be a result of international politics, while, in turn, private parties enable the provision of public services (Tikk, 2011). In short, public and private
interests overlap and mutual dependencies increase, so that both public and private actors are needed for comprehensive cyber security management.

In practice, much of the existing collaboration focuses on the sharing of processed information between various parties (see Carr, 2016). A US case study proves that cyber intelligence-sharing communities are often structured around industry sectors (Jasper, 2017). Examples include the Information Sharing and Analysis Center (ISAC) and the Information Sharing and Analysis Organization (ISAO). These networks facilitate the dissemination of collected and analyzed intelligence towards governments and private sector parties (Jasper, 2017). Collective research on how to tackle novel intelligence challenges is another example of public-private collaboration (see Vogel et al., 2017).

While these are noble initiatives, the cooperation between public and private parties is not always effective or successful. A range of limitations has been identified. For instance, intelligence sharing can be complicated by restrictions on the dissemination of classified information, so that it is unclear what can be shared with whom (Jasper, 2017; Strachan-Morris, 2009; Trim, 2001). Additionally, public and private actors have very different priorities, respectively the provision of basic services and profit maximization, and therefore different expectations of the collaboration (Carr, 2016; Harknett & Stever, 2009; Trim, 2003; Vogel et al., 2017). Consequently, mutual trust may be absent or scarce (Jasper, 2017; Trim, 2001; Vogel et al., 2017). Case studies also report differences in the ways of working, norms, language use, formats, and systems (Jasper, 2017; Vogel et al., 2017). Lastly, even if intelligence is successfully collected, analyzed, and disseminated, it may be problematic to make it an elementary part of decision-making, which could render the effects of cyber intelligence collaboration still unsatisfactory (Jasper, 2017).

These limitations have led to several suggestions for improvement. Harknett and Stever (2009), for instance, recommend not to centralize structures in response to these challenges but to boost the coordination potential instead. Next, based on a longitudinal study of intelligence collaboration between industry, government, and academia, Vogel et al., (2017) derived empirically based best practices. Specifically, they found that adaptation and innovation were essential elements of a flexible approach, which enabled the introduction of small changes to ensure the continued motivation of participants and to advance their mutual collaboration.

While these studies shed light on the need and motivations for private engagement in cyber intelligence collaborations and identifies some key challenges and possible resolutions, it portrays a uniform image of public-private networks in this field. Strikingly, cyber intelligence networks with only private actors are virtually ignored. Moreover, some questions as “How does such cooperation arise? How frequently and what form does it take?
Who authorizes it and arranges it?” remain often unaddressed in the current literature (Lefebvre, 2003, p. 533). In this study, we bring these elements together by exploring public, private, and public-private cyber intelligence networks. Given our focus on networks, our cases all have at least three active parties, which excludes intelligence collaboration in partnerships (cf. Lasoen, 2017). Additionally, we only focus on domestic collaboration to limit the scope of this research. These boundary conditions enable us to describe ideal-typical networks in some detail. Specifically, we identify four types of networks (one public, one private, and two public-private networks) and briefly outline the characteristics of these networks. On the basis of our exploratory analysis, we are enabled to answer our research question as to what types of cyber intelligence networks can be distinguished and which characteristics these networks have.

**Methods**

The case for this research is the broad range of cyber intelligence networks in the Netherlands. The Netherlands is a technologically advanced country, in which both public and private organizations are increasingly dependent upon digital information systems and infrastructures (see Claver, 2018). Since the country is facing considerable cyber security threats, a strong consensus on the need for cyber intelligence collaboration has emerged (NCTV, 2017). As an exploratory case study, our focus on the cyber intelligence networks in one country (i.e. the Netherlands) enables an in-depth and careful description of the phenomenon under study in this context. The select focus may subsequently be corroborated or refined by cross-case comparisons and quantitative studies. Yet, although our empirical scope is limited to the Dutch context, the theoretical implications of this study may be of broader relevance.

To answer our research question, we collected data through a combination of data collection methods. Firstly, we conducted nine interviews with prominent figures and network participants in the cyber intelligence field. All respondents played a role in a cyber intelligence network (and sometimes in multiple networks) and we made sure that we interviewed people of both public and private organizations. On average, an interview lasted sixty minutes. All but one of these interviews could be recorded, while the respondent of the unrecorded interview received a transcript on the basis of notes taken during the interview. Secondly, we asked respondents to provide us with documents pertaining to cyber intelligence networks. Even though the field is known to be relatively closed to external scrutiny (see Carr, 2016; Claver, 2018), we received internal documents which described network goals and entry requirements as well as prescriptions of behaviors of network participants. Lastly, we searched for open source information regarding cyber intelligence networks in the Netherlands to complement
our data. Government websites and reports, in particular, proved insightful in this regard. The combination of these empirical sources ensured triangulation of our data.

Upon analysis of this data, we found a variety of cyber intelligence networks, some of which comprised of only private or only public actors, while others had a public-private nature. Initially, our analysis was data-driven: we derived relevant network aspects that featured in the data and were deemed important by cyber intelligence personnel. After having identified a range of network aspects, we went back to the literature to find out which network aspects had earlier been suggested to be relevant. This reiterative moving between data and theory helped us to pool concepts together in order to select only the most important aspects (see Ketokivi & Mantere, 2010). The following aspects remained: history, activities, governance structure, communication frequency, goal consensus, member commitment, and perceived results. After analyzing the range of cyber intelligence networks on these aspects, we noticed that several networks proved analytically very similar. We pooled these together until four cyber intelligence networks remained: centralized, business, operational, and local networks. In the next section, we describe each of these networks in turn by providing the relevant information on an ideal-typical case of every network.

Findings

Our data enables us to construct a typology of cyber intelligence networks (see Table 1). Four types of networks can be distinguished: the centralized network, the business network, the operational network, and the local network.

Centralized network

History
The centralized network typically emerges through top-down intervention and is founded on the basis of a governmental wish to improve the cyber

| Table 1. A typology of cyber intelligence networks. |
|---------------------------------|-----------------|-----------------|-----------------|-----------------|
| History                         | Centralized     | Business        | Operational     | Local           |
| Activities                      | Top-down        | Top-down        | Bottom-up       | Bottom-up       |
| Governance structure            | Administrated   | Collective action | Collective action | Administrated   |
| Communication frequency         | Low             | Hierarchical    | Shared          | Administrated   |
| Goal consensus                  | Low to medium   | Low             | High            | Medium          |
| Member commitment               | Low             | Low             | High            | Medium          |
| Perceived results               | Low             | Medium          | High            | High            |
| Composition in our cases        | Public-private  | Public-private  | Public          | Private         |
security of public services. Specifically, it is introduced to centralize cyber intelligence sharing among public and private organizations in designated sectors. In practice, the centralized network therefore predominantly ‘brings the separate images [of its members] together to construct shared situational awareness’ (Interview, centralized network member). Every sector has its own, similar, centralized network, consisting of both public and private organizations working in the same field of operations.

Activities
The activities in the centralized network consist primarily of ‘the exchange of intelligence’ (Interview, centralized network member). For instance, participants share which cyber intelligence threats they have recently faced and which cyber incidents have occurred. Participants may also share their experience on which security mechanisms proved effective or failed as well as give and receive advice on how they can increase the cyber resilience of their organizations.

Governance structure
As a medium-sized network, the centralized network makes use of an administrator-led governance structure, which means that the initiating public party has a supervising and mediating role in bringing parties together, maintaining the relationships in the network, and facilitating the intelligence-sharing activities. Even though there is a founding organization, there is no formal hierarchy in this network, as its members ‘really strive to meet on an equal level’ (Interview, centralized network member). Both public and private parties have an identical position and similar decision-making powers.

Communication frequency
The number of face-to-face meetings in the network are quite low. For example, network participants gather only once every six to eight weeks, but even when there are meetings, members are not always attending. Some of the participants have informal contact from time to time as well, but the overall frequency with which intelligence is shared among partners remains relatively limited, so that members ‘do not know each other well, as they see each other so rarely’ (Interview, centralized network member).

Goal consensus
The degree of goal consensus is low to medium. The overarching goal of the centralized network is to improve the sharing of cyber intelligence between relevant organizations in a sector, so that these parties can inform each other if there is a cyber-leak, a breach, or a full-scale crisis. However, in practice, the overarching goal regularly disappears to the background as members admit that ‘ultimately, they are in this collaboration primarily for their own
organization’ (Interview, centralized network member). In practice, some private sector participants are fierce competitors outside of the network and therefore consider their individual goal ahead of the network goal. Relatedly, there are incompatible motivations between public and private participants: public agencies aim to improve their own cyber intelligence positions, while private parties ultimately wish to enhance their profits and merely see the network as a means to this end.

**Member commitment**

The participants in the centralized network identify stronger with their own organizations than with the network. Their commitment to the network and involvement in its activities are relatively low and one member reports that ‘people can easily withdraw from the collaboration’ (Interview, centralized network member). In practice, ideas and initiatives regularly amount to nothing due to different prioritizations of members, which indicates that the network is not able to attract strong commitments to achieve shared ideas and also shows that organizational members are primarily concerned with the relevance of the network to their own organizations’ aims.

**Perceived results**

Network participants generally perceive the results of the centralized network as limited. Although all parties are formally equal, there are considerable differences among organizations, as some have much more advanced cyber security measures, knowledge, and policies than others. Additionally, the public-private exchange of cyber intelligence is complicated, because private organizations are afraid that their reports of cyber intelligence will induce new or more strict regulation, while public organizations face confidentiality questions and do not completely trust their private partners. The results, therefore, often do not meet initial expectations and ‘initiatives emerging here tend to get off track’ (Interview, centralized network member).

**Business network**

**History**

The business network is ‘more or less imposed at the highest level’ (Interview, business network member) to establish the exchange of cyber intelligence and cyber expertise between a requesting, public party and several private service-providing organizations. As the public organization pays the others in return, this organization defines the character of the collaboration, its emergence, and its possible abandonment, rendering this network top-down in character.
Activities
The activities of the business network consist of several forms of collective action, but the exact content of the support is determined by the requesting party, since the needs of this organization underpin the formation and activities of the business network. For instance, one public organization ‘participated with a few companies as a team in an [international] training exercise’ to test its cyber resilience (Interview, business network member). In addition, network participants collectively implement cyber security measures as well as share intelligence.

Governance structure
The business network is medium-sized and has a clear leading organization. Since the public agency is reimbursing the other organizations in exchange for their expertise and help, the network is very hierarchical: ‘it is just like a customer calling for a job, […] just like a commercial order’ (Interview, business network member). All activities are executed to serve the purposes of this leading organization and the network might be changed or dissolved by this leading agency, which renders network participants unequal.

Communication frequency
Face-to-face meetings take place every six to eight weeks. During these meetings, communication is often unidirectional. Intelligence flows from the private organizations towards the public organization, while this public agency ‘cannot share [its intelligence] with the others’ in turn (Interview, business network member).

Goal consensus
There is relatively low goal consensus in the business network. The requesting party aims to improve its cyber intelligence position and wishes to enhance its cyber security, while the hired parties mainly aim to make a profit. Regardless of there being ‘much goodwill and awareness of the great cyber problem’ (Interview, business network member), the goals of the service-providing organizations differ considerably from the principal’s goals in the business network.

Member commitment
Members do not commit strongly to the network. They identify themselves rather with their own organization than with the business network which serves primarily to serve the different organizational interests of the network participants involved. Private-sector participants recognize that their involvement depends solely on the profit opportunities of their own organization for which their integration in the overarching network is only a means. Although, once committed, membership ‘is no longer without obligations’
(Interview, business network member), the lack of a shared purpose reduces members’ loyalty to the network.

**Perceived results**
The perceived effectiveness of this network is medium. While the supplying organizations make a profit and thereby achieve successful results from their organizations’ perspectives, the requesting organization judges the results by very different standards and is not always completely satisfied. The diverging goals in this network mean that its outcomes are rarely perceived as unequivocally successful by the public agency, so that it wishes to ‘become more familiar with private companies’ and to ‘explore the direction in which the collaboration should develop’ (Interview, business network member).

**Operational network**

**History**
The operational network emerges through bottom-up endeavors. It is the product of cyber intelligence experts of different public organizations recognizing shared operational challenges and deciding to establish a network organization to institutionalize their collaboration. As a member of one operational network recalls: ‘We really started operationally together […] We knew we were working on the same goals, making the government cyber-resilient, and we thought: let’s do this together’ (Interview, operational network member). In this case, they quickly received support from their employers, which formalized the network.

**Activities**
Members in the operational network regularly ask themselves ‘why do we exist?’ and subsequently decide to aim for high-level collaboration (Interview, operational network member). Thus, they do not solely exchange relevant cyber intelligence, but also increase the resilience and efficiency of each other’s organizations by formulating ‘best practices’ and identifying how these can be implemented in the cyber systems of their respective organizations.

**Governance structure**
The governance structure of the operational network is shared, which means that there is a very flat and decentralized network structure. This is made possible by the small size of the network in which all participants are familiar on a personal level. The different members establish a steering committee for practical purposes, but remain in charge of all operational decisions, such as admission requirements for new entrants. In fact, potential new members face a ‘threshold to first ensure that new members will bring
something in turn’ (Interview, operational network member). Once admitted, new members are equal to the others, so that any hierarchical relation in the operational network remains absent.

**Goal consensus**
There is very high goal consensus in operational networks, as some members describe the network as ‘a unified entity’ (Interview, operational network member). In practice, the participants have formulated and written down clear network goals, which are supported by all members. These goals, however, merely reflect pre-existing, informal agreements on the cyber security needs of their organizations. Importantly, the organizations for which network participants work formally support these goals as well.

**Communication frequency**
The number of face-to-face meetings between members of operational networks are comparatively high. Indeed, members are characterized as ‘knowledgeable, enthusiastic, and willing to make time for it’ (Interview, operational network member). In one case, for instance, they met once every week. Network participants also communicate and collaborate extensively on an informal basis. They share relevant intelligence with each other outside of the formal network structure without much hesitation.

**Member commitment**
Network members identify more strongly with the operational network than with their own organization and feel a strong commitment to network goals. The network is attractive to members due to its high aims and high-level collective actions. The shared experience of establishing and institutionalizing the network generates considerable participant loyalty to it as well. Additionally, frequent collaboration on a formal and informal basis between participants further helps to draw allegiance of members to the network instead of to the respective organizations involved. One member concluded: ‘I am not here as a representative of [my own organization]; we are here as a network collaboration’ (Interview, operational network member).

**Perceived results**
Members of the operational network perceive the network’s effects as very beneficial. The aims are often reached due to both individual and organizational commitments, the clarity of the formulated goals, and intensive collaboration efforts. Network participants ‘share a lot of information with each other and make collective [intelligence] products of it’ (Interview, operational network member). The network, thus, enjoys a virtuous cycle, since beneficial results, participant commitment, and collective endeavors reinforce each other.
Local network

History
The local network has a history of bottom-up commitment as well. It is typically founded by a group of local, private organizations that recognize a shared interest in ‘sharing best practices’ on cyber security and decide to establish this network to that end (Interview, local network member). Informal intelligence-sharing has often been ongoing for a long time, resulting in the eventual creation of a cyber intelligence network when the need for institutionalization of these practices emerges.

Activities
Members of the local network solely aim to share relevant cyber intelligence with each other. This intelligence may concern cyber threats, possible security-enhancing measures, or ensuring greater resilience. Typically, ‘during meetings, best practices are discussed’ as well as experiences and questions (Interview, local network member). Since the participants are geographically located nearby each other, they visit each other also ad hoc in case of emergencies.

Governance structure
The governance structure of the local network is rather decentralized. As the network has many participants, the practical decision to appoint ‘a chair who sends out the agenda’ has been made in order to maintain the network relations and facilitate the meetings, but this chair does not have any formal power and ‘the agenda is collectively set’ (Interview, local network member). Irrespective of the administrative role of the chair, everyone remains equal and decisions are made by all members together in a fairly democratic manner.

Communication frequency
The intensity of face-to-face meetings in the local network is medium. In one case, members met only once every ten weeks to share their intelligence in the network. However, there are many informal contacts between different members and members have a long history of collaboration, which means that their interactions are considerable, even though not always taking place in the network context. Due to recurring interactions, the ‘initial reluctance’ to share intelligence among each other is slowly replaced by the awareness that ‘things that are confidential, remain confidential’ (Interview, local network member).
**Goal consensus**

The goal consensus in the network is quite high, as all members are ‘regional private producers’ (Interview, local network member). Relatedly, the network goal has been established with the founding of the network and prescribes the common intent to share cyber intelligence among members. Although this goal is broad and not operationalized, members value it highly and are willing to disregard their specific organizational interests when gathering in the network context.

**Member commitment**

Whereas the frequency of face-to-face meetings in the local network is relatively limited, members nevertheless identify with the network rather than with their own organizations when they convene. This counterintuitive fact may be explained by their involvement in the establishment of the network and their extensive informal interactions. One member states that ‘trust is the basis of this groups, so you can share anything, and since [membership] remains local, [confidentiality] is guaranteed’ (Interview, local network member).

**Perceived results**

Members of the local network perceive the network as successful. The modest goal of cyber intelligence sharing is achieved due to a strong commitment of members and a willingness to set aside organizational interests in pursuit of the overall network goal. Strong informal and ad hoc interactions, which are not taking place within the network context but are nevertheless encouraged by it, also turn out to be very relevant for the organizations involved. Participants, thus, ‘get out of it what they had planned, so in that regard, the goal is achieved’ (Interview, local network member).

**Discussion**

In our analysis of different types of cyber intelligence networks, we identified four ideal-typical networks: centralized, business, operational, and local networks. For every network type, we have provided basic information regarding the network’s history, activities, governance structure, communication frequency, goal consensus, member commitment, and perceived results. Consequently, the similarities and differences between the networks become clear. The findings of this study enable us to spell out some specific contributions that we make to the literature on cyber intelligence collaboration.

Firstly, we demonstrate that collaboration efforts in cyber security management cannot be pooled into one, uniform network type, since cyber intelligence networks have different characteristics. While existing studies have identified a range of challenges and outcomes of cyber security
networks (e.g. Carr, 2016; Harknett & Stever, 2009; Jasper, 2017; Trim, 2003), we suggest that it is fruitful to distinguish between separate types of networks in order to make better sense of these challenges and outcomes. For example, while motivations of partners more or less align in operational and local cyber security networks, they may widely vary in business networks. The challenge of different priorities, as suggested by some authors (Harknett & Stever, 2009; Trim, 2003), will therefore specifically apply to this latter type of collaboration. By extension, the added value of proposed resolutions depends on the type of network under study. Some networks may benefit from adaptation and innovation (see Vogel et al., 2017), but others may in fact derive benefits from more formalization and centralization to ensure that the network lasts, even when key organizational representatives or founders leave (e.g. this may apply to operational networks). Our identification of four ideal-types is not conclusive, so other types of networks may be added to the typology in the future to refine our analysis. In general, we claim that the network type influences the challenges and outcomes of cyber intelligence cooperation.

Secondly, our research shifts the attention from public cyber intelligence agencies to private actors. While widely recognized as an important set of actors in cyber security management (Carr, 2016; Shore, 2015; Tikk, 2011), the initial focus of many intelligence studies is on public agencies instead. For instance, much research still focuses only on the collaboration between public intelligence agencies on the national and international levels (e.g. Cozine, 2016; James et al., 2017; Parkes, 2017; Seagle, 2015; Vestermark, 2017). Moreover, research that does have an interest in private sector engagement in cyber intelligence collaboration uses a public-private lens (e.g. Carr, 2016; Jasper, 2017; Trim, 2003). Networks with only private sector participants are therefore commonly ignored in existing studies. Nevertheless, we find that some networks (i.e. local networks) consist exclusively of private parties. Interestingly, these networks have been rated in positive terms and achieved beneficial results. This is not to say that public agencies are irrelevant to tackling cyber intelligence threats, but emphasizes the need to examine private sector endeavors more extensively. Possibly, lessons can be learned from successful private cyber security networks that may be extended to public sector efforts.

Thirdly, public-private collaborations typically emerge after top-down initiatives, as demonstrated in our centralized and business cyber intelligence networks. Examples in the literature of this include Information Sharing and Advisory Councils (ISACs), the National Cyber Security Alliance, and the National Cybersecurity and Communications Integration Center (Harknett & Stever, 2009; Jasper, 2017). Although reflective of governmental wishes to make use of differentiated expertise, our study shows that top-down endeavors may not lead to the strongest participant commitment or the highest
perceived results. Instead, we identified networks emerging from the bottom-up as well (i.e. operational and local networks), which were generally less hierarchical and formal, but perceived to be more successful. Our limited empirical scope does not allow for sweeping general conclusions, but these findings suggest that the full potential of public-private networks may not be harvested at the moment. Instead, cyber security may be improved by inducing and encouraging more bottom-up explorations of cyber intelligence networks.

**Shortcomings and future research**

While our research offers theoretical contributions and practical insights, there are several limitations to this study, which may be addressed in future research. Firstly, our study only focuses on cyber intelligence collaboration in The Netherlands. This country is not necessarily representative for collaborations in this domain across the globe (Claver, 2018). For instance, we did not find a collaboration between academia and public or private organizations on cyber intelligence (cf. Pascovich, 2017; Vogel et al., 2017). This does not necessarily undermine the theoretical implications of our research, but is an inevitable consequence of the exploratory nature of the study. In fact, our study provides a provisional typology which may be refined and expanded by future research. To do so, we recommend follow-up studies in different countries, across different economic sectors, and in transnational contexts to gain a more comprehensive understanding of cross-sector cyber security networks. Relatedly, the intelligence domain is developing at a fast pace, with many new networks emerging. Future studies may also look into the lifecycles of these networks and attempt to explain more specifically which networks thrive and succeed in the long term as well as which networks fail and dissolve over time.

Next, to set boundaries to our research, we only focused on cyber intelligence collaboration in networks consisting of at least three organizations. This means that (business) partnerships fell out of the scope of this research (cf. Lasoen, 2017). Follow-up research could identify the specific histories, characteristics, and achievements of these partnerships to complement our research. In addition, our research indicates the important role that boundary-spanners (or liaisons) play in establishing and enacting collaboration in the cyber domain. This is equivalent to (physical) emergency management networks, in which close collaboration between individuals often proves to be a prelude to effective inter-organizational collaboration (see Kalkman & De Waard, 2017; Kalkman & Groenewegen, 2018). More research into how individual relations foster network emergence and network success seems promising.
Conclusion

There is broad academic consensus that cyber security threats are increasing and diversifying, ranging from cyber-terrorism and cyber-attacks to theft and sabotage. In response, public and private organizations have to improve their cyber intelligence position in order to be able to successfully assess these cyber threats and protect themselves. Currently, collaboration across organizational boundaries is believed to be an essential element of cyber intelligence. In our study, we analyzed cyber intelligence networks to provide an overview of the different types of networks that exist and their specific characteristics. We constructed a typology of four cyber intelligence networks: centralized, business, operational, and local networks. These networks vary in terms of their history, activities, governance structure, communication frequency, goal consensus, member commitment, and perceived results. The typology shows that, when one discusses cyber intelligence networks, it is important to specify which type of network one has studied. These findings may also help practitioners to reflect on the most appropriate type of network to establish or support.

Practical implications

Specifically, the networks with the highest experienced results are the operational and local networks, which both emerged bottom-up in contrast to the other network types. Yet, even though the centralized network may not be the most appropriate network mode under all circumstances, most cyber security networks still fall within this category. This does not mean that governments should shift all their resources to inducing bottom-up initiatives. These networks may be instable as they generally lack formalized procedures and agreements. As such, these cyber networks are likely to be unable to host a large group of public and private organizations with diverse interests, as is the case in centralized networks. Nevertheless, one collaboration strategy does not necessarily exclude the others. In fact, we suggest that multiple networks can coexist and overlap. The current absence of more decentralized and bottom-up cross-sectoral networks triggers the wish to experiment with this type of collaboration. For instance, public organizations can incentivize their personnel to explore low-level network collaborations with a variety of public and private partners. In addition, members of cyber intelligence networks may use our typology to identify what type of networks they are participating in, what the risks are to these networks, and how they can respond to looming challenges. As such, they can use our findings to build a more resilient cyber intelligence network. In general, we hope that our typology of cyber intelligence networks encourages researchers and
practitioners alike to explore and experiment with the different types of intelligence networks so to ultimately improve cyber security.

Note

1. In this research, we use ‘cyber intelligence networks’ and ‘cyber security networks’ interchangeably on the assumption that cyber intelligence networks aim to enhance cyber security, while cyber security networks require the sharing and usage of cyber intelligence to be operational (see Mattern et al., 2014).

Notes on contributors

Jori Pascal Kalkman is assistant professor at the Netherlands Defence Academy. During his PhD, he investigated the collaboration between military and civilian organizations in crisis and disaster management. In his research, he relies primarily on literature from organization sciences and public administration.

Lotte Wieskamp holds a Master’s degree in Organization Sciences from the VU University, Amsterdam. During her Master’s thesis research, she analyzed cyber intelligence collaboration between public and private organizations in the Netherlands. Currently, she works as Advisor on Cyber Security and Privacy.

References

Allison, G. T. (1971). Essence of decision: Explaining the Cuban missile crisis. New York, NY: HarperCollins Publishers.

Carr, M. (2016). Public–Private partnerships in national cyber-security strategies. *International Affairs, 92*(1), 43–62. doi: 10.1111/inta.2016.92.issue-1

Claver, A. (2018). Governance of cyber warfare in the Netherlands: An exploratory investigation. *The International Journal of Intelligence, Security, and Public Affairs, 20*(2), 155–180. doi: 10.1080/23800992.2018.1484235

Clough, C. (2004). Quid pro quo: The challenges of international strategic intelligence cooperation. *International Journal of Intelligence and CounterIntelligence, 17*(4), 601–613. doi: 10.1080/08850600490446736

Cozine, K. (2016). Fragmentation and interdependency: Border security intelligence in North America and Europe. *The International Journal of Intelligence, Security, and Public Affairs, 18*(3), 175–197. doi: 10.1080/23800992.2016.1242268

U. S. DoD (2016). Joint publication 1-02: Department of defense dictionary of military and associated terms. Washington, D.C.: Joint Staff.

Gill, P., & Phythian, M. (2006). *Intelligence in an insecure world.* Cambridge, MA: Polity Press.

Gill, P., & Phythian, M. (2016). What is intelligence studies? *The International Journal of Intelligence, Security, and Public Affairs, 18*(1), 5–19. doi: 10.1080/23800992.2016.1150679

Harknett, R. J., & Stever, J. A. (2009). The cybersecurity triad: Government, private sector partners, and the engaged cybersecurity citizen. *Journal of Homeland Security and Emergency Management, 6*(1), article 79.
James, A., Phythian, M., Wadie, F., & Richards, J. (2017). The road not taken: Understanding barriers to the development of police intelligence practice. *The International Journal of Intelligence, Security, and Public Affairs*, 19(2), 77–91. doi:10.1080/23800992.2017.1336395

Jasper, S. E. (2017). U.S. cyber threat intelligence sharing frameworks. *International Journal of Intelligence and CounterIntelligence*, 30(1), 53–65. doi:10.1080/08850607.2016.1230701

Kalkman, J. P., & De Waard, E. J. (2017). Inter-organizational disaster management projects: Finding the middle way between trust and control. *International Journal of Project Management*, 35(5), 889–899. doi:10.1016/j.ijproman.2016.09.013

Kalkman, J. P., & Groenewegen, P. (2018). On frontline workers as bureau-political actors: The case of civil–military crisis management. *Administration & Society*, Online first doi:10.1177/0095399718780581.

Kalkman, J. P., Kerstholt, J. H., & Roelofs, M. (2018). Crisis response team decision-making as a bureau-political process. *Journal of Contingencies and Crisis Management*, 26(4), 480–490. doi:10.1111/jccm.2018.26.issue-4

Ketokivi, M., & Mantere, S. (2010). Two strategies for inductive reasoning in organizational research. *The Academy of Management Review*, 35, 315–333.

Lassen, K. L. (2017). For Belgian eyes only: Intelligence cooperation in Belgium. *International Journal of Intelligence and CounterIntelligence*, 30(3), 464–490. doi:10.1080/08850607.2017.1297110

Lefevre, S. (2003). The difficulties and dilemmas of international intelligence cooperation. *International Journal of Intelligence and CounterIntelligence*, 16(4), 527–542. doi:10.1080/716100467

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, CA: RAND Corporation.

Manjikian, M. (2015). But my hands are clean: The ethics of intelligence sharing and the problem of complicity. *International Journal of Intelligence and CounterIntelligence*, 28(4), 692–709. doi:10.1080/08850607.2015.1051411

Mattern, T., Felker, J., Borum, R., & Bamford, G. (2014). Operational levels of cyber intelligence. *International Journal of Intelligence and CounterIntelligence*, 27(4), 702–719. doi:10.1080/08850607.2014.924811

Meakins, J. I. (2018). Squabbling Siloviki: Factionalism within Russia’s security services. *International Journal of Intelligence and CounterIntelligence*, 31(2), 235–270. doi:10.1080/08850607.2018.1417525

NCTV. (2017). *Cybersecuritybeeld Nederland CSBN2017*. Den Haag, The Netherlands: Author.

Parkes, A. (2017). Lessons through reform: Australia’s security intelligence. *The International Journal of Intelligence, Security, and Public Affairs*, 19(3), 157–170. doi:10.1080/23800992.2017.1384675

Pascovich, E. (2017). Security and intelligence studies in Israel. *The International Journal of Intelligence, Security, and Public Affairs*, 19(2), 134–148. doi:10.1080/23800992.2017.1336402

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and CounterIntelligence*, 26(3), 453–481. doi:10.1080/08850607.2013.780552

Seagle, A. N. (2015). Intelligence sharing practices within NATO: An english school perspective. *International Journal of Intelligence and CounterIntelligence*, 28(3), 557–577. doi:10.1080/08850607.2015.1022468

Shore, J. J. M. (2015). An obligation to act: Holding government accountable for critical infrastructure cyber security. *International Journal of Intelligence and CounterIntelligence*, 28(2), 236–251. doi:10.1080/08850607.2014.962356
Sloan, S. (2006). The new terrorist threat environment. Continuity and change in counter-terrorism intelligence. In P. Katona, M. D. Intriligator & J. P. Sullivan (Eds.), Countering terrorism and WMD: Creating a global counter-terrorism network (pp. 199–211). New York, NY: Routledge.

Stouder, M. D., & Gallagher, S. (2013). Crafting operational counterintelligence strategy: A guide for managers. International Journal of Intelligence and CounterIntelligence, 26(3), 583–596. doi:10.1080/08850607.2013.780560

Strachan-Morris, D. (2009). The future of civil–military intelligence cooperation based on lessons learned in Iraq. Intelligence and National Security, 24(2), 257–274. doi:10.1080/02684520902819669

Tikk, E. (2011). Ten rules for cyber security. Survival, 53(3), 119–132. doi:10.1080/00396338.2011.571016

Trim, P. R. J. (2001). Public–Private partnerships in the defence industry and the extended corporate intelligence and national security model. Strategic Change, 10, 49–58. doi:10.1002/(ISSN)1099-1697

Trim, P. R. J. (2003). Public and private sector cooperation in counteracting cyberterrorism. International Journal of Intelligence and CounterIntelligence, 16(4), 594–608. doi:10.1080/026845203200032004

Velasco, F. (2016). Editorial. The International Journal of Intelligence, Security, and Public Affairs, 18(1), 1–4. doi:10.1080/23800992.2016.1150681

Velasco, F. (2017). Intelligence as a bet. The International Journal of Intelligence, Security, and Public Affairs, 19(1), 1. doi:10.1080/23800992.2017.1290372

Vestermark, T. (2017). International intelligence Liaison in the Afghan theatre of war: Strategic interests and hierarchical relations. The International Journal of Intelligence, Security, and Public Affairs, 19(2), 112–133. doi:10.1080/23800992.2017.1336400

Vogel, K. M., Jameson, J. K., Tyler, B. B., Joines, S., Evans, B. M., & Rendon, H. (2017). The importance of organizational innovation and adaptation in building academic–industry–intelligence collaboration: Observations from the laboratory for analytic sciences. The International Journal of Intelligence, Security, and Public Affairs, 19(3), 171–196. doi:10.1080/23800992.2017.1384676