JOURNAL OF CYBERSECURITY

*Journal of Cybersecurity*, 2018, 1–16
doi: 10.1093/cybsec/tyy008
Research paper

Research paper

# Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views

**Aviram Zrahia** *

The Blavatnik Interdisciplinary Cyber Research Center, Tel Aviv University, Tel Aviv, 6997801, Israel

*Corresponding author. E-mail: aviramzrahia@mail.tau.ac.il

Received 19 November 2017; revised 3 August 2018; accepted 2 October 2018

## Abstract

Real-time actionable threat intelligence is an emerging defense concept focused on detection and mitigation of cyber threats. The sharing of this information between parties reduces duplication of effort and allows one organization's detection to become another's prevention. Although there are deployments of threat intelligence sharing across different sectors, the partnerships formed between vendors in the cybersecurity market space have a significant coopetition attribute. This article aims to improve the understanding of those relationships through an empirical study by answering questions such as the following. What insights can be derived from the network structure formed between the vendors? What are the characteristics of the established relationships? Are there any properties that are common among sharing firms? The research is based on a uniquely coded dataset of vendors and their threat-sharing relationships studied from industry, dyadic, and firm perspectives. The methodology relies on a deductive-reasoning top-down approach and utilizes graph visualization and statistical analysis tools. The key findings are as follows: (i) the cybersecurity industry exhibits a small-world structure associated with communities, suitable for effective intelligence sharing, (ii) the collaborations are characterized by coopetition between loosely integrated complementary solutions, and (iii) the number of threat-sharing relationships of a firm is positively associated with its innovation level; the effect size is nearly three times stronger among publicly traded companies than privately held companies. The article aims to contribute to both domain knowledge and methodology by discussing a distinctive statistical and visual view of the analyzed ecosystem in the context of cyberspace and integrating multidisciplinary theoretical constructs into the researched domain from different study perspectives. The results may be used by security vendors, policy decision makers, and regulation authorities to assess the market dynamics, and the methodology and lessons can be generalized and applied to other domains.

**Key words**: threat intelligence; coopetition; network structure; information sharing; cybersecurity; security management

## Introduction

The world is facing the continuous challenge of fighting cyber threats from offenders motivated by cybercrime, cyberwarfare, and cyberterrorism. When engaging a target, attackers have many asymmetric characteristics that work to their benefit. A notable example is the use of knowledge sharing between attackers to establish technological and time-to-market advantages [1], while in many cases the defenders operate in silos. The former director of the NSA, Gen. Keith B. Alexander, referred to this aspect in his keynote speech during the cybersecurity RSA conference of 2011,[1] stating that: "Securing our nation's network is a team sport".

Technology and culture allow sharing between people and organizations, from social networks, through collaborative code

writing, to crowdsourcing in the cybersecurity space. One of the emerging implementations of this trend is the sharing of real-time actionable information referred to as Cyber Threat Intelligence (CTI). CTI is a dynamic feed of threat- or attack-related objects that are utilized for decision making or enforcement at the receiving end. Deploying information sharing between different organizations represents a collaborative effort to improve a cyber defense posture by leveraging the capabilities, knowledge, and experience of the broader community. The technology-related outcome is reduced duplication of effort, and it enables one organization's detection to become another organization's prevention.

The existing CTI-related body of knowledge (BoK) is focused on three key areas. The first area is the formats of CTI objects and sharing protocols [2, 3]. The second is the technological and structural forms of CTI sharing initiatives [4–7]. This study relates to the third and the least-researched BoK area: the non-technological social aspects and challenges that sharing presents to organizations [8–10].

Although there are many deployments of threat intelligence sharing across different sectors, the relationships formed between cybersecurity vendors have an interesting attribute. Since the shared information is closely related to the core business of the firms, it presents a unique challenge of combining collaboration with competition, which has been referred to as coopetition. Social challenges are larger when the parties are direct competitors or have other conflicts of interest. The sharing entities need to maintain their competitive edge, protect their commercial interests and intellectual property, and comply with laws and regulations, while providing a meaningful amount and quality of shared data to make the alliance useful. The financial aspects of security information sharing have been studied by Gordon *et al.* [11], Tosh *et al.* [12], Gal-Or and Ghose [13], and others, but no research so far has analyzed it from a cybersecurity vendor perspective, where the coopetition characteristic is vividly present.

This article aims to improve the understanding of threat intelligence sharing between cybersecurity vendors through an empirical study of the organizational characteristics, the dyadic relationships, and the network structure of the formed ecosystem. The insights provided are increasingly relevant given the growing trend of CTI sharing and the evolving number of vendor relationships. Some of the questions asked and answered in this article are: What insights can be derived from the network structure properties of the formed ecosystem? What are the characteristics of the established relationships and how do they reflect on the industry? Are there any properties common to sharing firms or associations between sharing behaviors and real-world market success?

The article considers the three theoretical constructs of network structure, coopetition, and information sharing, viewed from the three complementary perspectives of industry, relationship, and firm, respectively. The study analyzes a uniquely collected and coded dataset of vendors and their announced threat-sharing relationships during the years 2013–16 (Q1). The methodology is based on a deductive reasoning top-down approach, which is used to extract hypotheses from existing literature theories and match data-driven observations based on network (graph) theory and statistics against them. The findings are discussed in the context of the researched domain and transformed into conclusions.

From a network perspective, key features learned from graph theory studies were used to characterize the formed structure as demonstrated in empirical network research [14, 15]. The result indicates that the analyzed network exhibits small-world characteristics associated with a modular (community) structure, suitable for effective threat intelligence sharing. Mapping the network connected components and presenting them as a bow tie diagram revealed nodes within this structure that are key to distribution of intelligence; this mapping assumed knowledge spillovers occur [16]. The clustering attribute seemingly creates a competitive advantage for the sharing firms, compared to non-sharing vendors, as proposed by Brandenburger and Nalebuff [17]. In addition, the community structure allows for threat intelligence commoditization within cluster members, and thus the shift of competitive focus toward other product differentiating aspects. The small-world and community structure features of the analyzed network resemble empirical findings from studies of research and development (R&D) networks [14, 15, 18–20]. However, the established threat-sharing relationships are not R&D collaborations per se, which benefit greatly from lowering R&D costs, but rather are information exchange initiatives. Therefore, it appears that other motivations, such as societal welfare or indirect financial gains, drive the cooperation in this market.

The study also confirms that the relationships represent coopetition between loosely integrated complementary solution types. One might think that companies with competing products in the same market category will not tend to cooperate. However, the demonstrated competitive nature is in line with arguments made by Gal-Or and Ghose [13] who found sharing to be more beneficial when product substitutability is higher, which implies a higher competitiveness of the industry. For the solution-type characteristics, the literature indicates that complementary skills and capabilities of two cooperating companies are significant factors supporting collaboration success [21], and combined knowledge is known to yield better results than individual knowledge [22]. From a resource-based view [23], high-quality CTI is essential for customer-base growth. However, access to uniquely identifiable intelligence requires customer-base growth to facilitate a broader attack landscape perspective. Therefore, sharing intelligence between security vendors becomes the means to overcome this catch-22 scenario[2] and could partially explain why sharing companies are ranked higher for innovation and success.

From a firm perspective, network properties were correlated with real-world organizational attributes to create a merged view of the industry and firm levels. The findings in this article indicate a positive association between the number of cooperative relationships of a firm (network degree) and its innovation level. This conclusion is in agreement with empirical studies in other domains that show correlations between network properties and success [24, 25] and with models suggesting that firms with prospecting strategies are more likely to engage in coopetition [26]. We found that publicly traded companies participate in threat intelligence sharing more than twice as much as privately held companies with a difference in correlation effect size of nearly threefold. These results are well inline with the literature. Previous studies have shown that publicly traded firms have higher rates of growth than privately held firms [27] as well as a better patent portfolios than their private counterparts; hence they are more innovative [28]. In addition, collaboration among large competing companies was found to yield large positive effects on technological diversity [29], explaining in part the higher rates of cooperation among publicly traded firms, which tend to be larger than private companies.

1 https://www.youtube.com/watch?v=7I-bZjd75VE

2 Coined by the American author Joseph Heller, the expression "catch-22" is often used to describe a paradoxical situation caused by contradictory rules

This study aims to contribute to knowledge by studying explicitly CTI sharing among vendors and by visualizing, analyzing, and discussing a uniquely coded novel dataset that contains cross-referenced vendor records and relationship records. It also contributes to methodology by mapping multidisciplinary literature constructs into the research domain from the network, dyad, and agent perspectives. The findings may be used by security vendors to assess the existing market dynamics, policy decision makers in all verticals to reconsider their sharing strategies, and regulation authorities to encourage CTI sharing.

The paper is organized as follows: the "Background" section covers the background of the CTI problem domain and the related literature. The "Research essentials" section describes the empirical dataset, methodology, and tools used in this research. The "Empirical results" section details the results on three levels of analysis: network, relationship, and firm. The "Discussion and conclusion" section discusses the findings in light of existing literature and summarizes the conclusions while offering additional perspectives on the subject.

## Background

The article uses three theoretical constructs from the literature to provoke discussion: network structure, coopetition, and information sharing. In this section, we cover the literature and technology background of the researched problem domain and define a key theory for each construct to inspire the hypotheses in "Empirical results" section .

### Cyber threat intelligence

In modern cyber threats, the attackers seem to have the upper hand. Regardless of their motivation, their engagement with the target has asymmetric attributes that work to their benefit. For example, they can try many times to penetrate the target and fail, whereas the defenders must always succeed; they can keep their anonymity,[3] but the defenders are mostly known and exposed; and they can severely impact targets with relatively limited resources. In addition, attackers often share innovative Advanced Persistent Threat (APT) methods[4] easily and rapidly through a flourishing, structured, anonymous community with internal order and supporting systems of financing and technology [1]. Overall, these trends reduce the effectiveness of traditional security mechanisms and create the need for new attack identification and mitigation defense concepts to be deployed in a seemingly never-ending arms race.

CTI is an emerging defense concept, which was broadly defined by Gartner as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard"[5]. According to Chismon and Ruks [30], CTI objects can be mapped into four subtypes based on their features and consumption point: strategic high-level information, consumed by the organization's board and management; operational information about specific upcoming attacks on the organization, consumed by security managers; Tactics Techniques and Procedures (TTPs), information on how threat actors are conducting attacks, consumed by the incident response team; and technical information feeds, often consumed automatically by enforcement or analysis systems.

The intelligence discussed in this article is categorized as technical and presented as a structured feed of constantly updated cyber-related data objects. This feed is processed either manually or automatically and used off-line or in real time for analysis or prevention at the receiving end. The content of this threat feed in typically delivered using a black-list/white-list methodology and includes Indicators of Compromise (IOCs) such as command and control server IP addresses, email addresses used for spamming or phishing, Botnet identification objects, and/or a list of compromised DNS servers. It may also contain a structured form of attack descriptors or other cyber-related information components as industry standards evolve. CTI objects are correlated at the receiving end with the organizational traffic and context to identify, alert, or block suspicious transactions or behaviors. The analysis can be performed manually by human cyber experts or automatically as part of a decision-point product such as Security Information and Event Management (SIEM) or an enforcement-point product such as Next-Gen Firewall[6].

In recent years, the cybersecurity industry has acknowledged the need for collaboration. Whereas attackers see the entire "battle field" by gaining access to multiple targets, each defender has a limited and mostly unique perspective of his environment. This perspective gap is one of the drivers for threat information exchange. Sharing CTI objects between different organizational entities is a collaborative effort to improve one's cyber defense posture by leveraging the capabilities, knowledge, and experience of the broader community. Adapting the community model for cyber defense and transforming from a paradigm of isolated organizations to a threat-information-sharing community leads to an increased level of information security [11]. As a result, various organizations have developed policies for sharing cyber-related information with outside parties, and many have already joined forces in a collaborative effort to fight the cyber war. Moreover, the importance of CTI sharing has been acknowledged by local and international regulatory and law enforcement bodies that promote this trend by means of incentives, guidelines, and legislation[7].

The existing CTI-related BoK is focused on three key areas. The first one is the format of CTI objects and sharing protocols. A key standardization effort used to describe the CTI objects and automate their sharing includes a family of protocols and languages named STIX™, TAXII™, and CyBOX™. The U.S. Department of Defense has adopted these standards, and further work to expand their capabilities is being done in both academia and industry[8]. Qamar *et al.* [3] created a Web Ontology Language (OWL) for networks, Common Vulnerabilities and Exposures (CVEs) and

3 Mostly referred to as the "attribution challenge", which is the difficulty of identifying the true source of a cyber-attack.

4 A collection of cyber-attack tools and methods, better known as Advanced Persistent Threats (APTs), aimed at a specific target and controlled by professional hackers in a way that makes it very difficult to identify and mitigate using standard security measures.

5 Gartner's definition of Threat Intelligence: https://www.gartner.com/doc/2487216/definition-threat-intelligence

6 A security information and event management (SIEM) is a single pane of glass that provides real-time analysis of alerts and events. A Next-Gen Firewall is a network platform that provides application-layer access control, integrated with additional network security capabilities.

7 A notable example is the Cybersecurity Information Sharing Act of 2015 (CISA) which legally protects private and public companies in the USA that choose to share cyber-related information with the authorities: https://www.congress.gov/bill/114th-congress/senate-bill/754

8 Oasis CTI Technical Committee is a community-driven standardization effort: https://www.oasis-open.org/committees/cti/

STIX™, which maps the shared knowledge with network architectural schematics, to analyze the impact of potential threats and attacks on the network. Burger *et al.* [2] claim the current ontologies are limited to present use-cases and offer an agnostic taxonomy for STIX™/TAXII™ and other formats that is aimed at identifying their inherent gaps and explaining their differences from a scientific perspective.

The second BoK area is the structure of CTI sharing initiatives. Irrespective of the ontology used, the sharing implementation may take different technological and structural forms. It could be based on a trusted clearance center (hub-and-spoke), deployed directly between two organizations (peer-to-peer), or sent only from one entity to another (source-subscriber).[9] Scholars have introduced frameworks for building cyber-related community sharing [5, 7, 31], as well as best-practice methodologies for deploying them [32], and an inventory of tools relevant to the exchange and processing of actionable information [6]. Furthermore, specific rather than generic sharing implementations have been studied; one has been suggested by Fransen *et al.* [4] to gain early insight into a nationwide large-scale societal threat.

The last BoK area, and the least researched so far, is related to non-technological social aspects and challenges that sharing presents to organizations. In many cases, sharing initiatives represent a shift in the organization's legacy information technology (IT) paradigm, and create a complex, multifaceted challenge to technology, law, organizational culture, privacy, and politics [10]. As noted by Ring [9], dues to these challenges, in many cases, entities fail to share threat intelligence within their own company, let alone outside it. Furthermore, the contributing members might be a small fraction of the participating community, creating a situation of free-riders, which needs to be amended with a model as offered by Liu *et al.* [8] for the FS-ISAC financial sharing initiative.[10] Naturally, social challenges are larger when the parties are direct competitors or have other conflicts of interest. The entities need to maintain their competitive edge, protect their commercial interests and intellectual property, and comply with laws and regulations, while providing a meaningful amount and quality of shared data to make the alliance useful. Throughout this study, we will refer to this situation as coopetition.

In recent years, a growing number of sharing alliances have emerged, linking individuals through social networks, companies within the same vertical market, entities across different sectors in the same geography, commercial and governmental bodies, and countries. Despite the described challenges, there are multiple examples for each type of sharing deployment mentioned. Notable examples include Facebook's crowd-sourced threat intelligence exchange app,[11] the US-based FS-ISAC collaboration within the financial vertical, the Advanced Cyber Security Center (ACSC) for cross-sector cooperation in the New England region, the CISCP initiative of the Department of Homeland Security (DHS) for sharing between critical infrastructure suppliers and the government,[12] and the CIICS automated information sharing among some of NATO's allied countries.

The sharing of threat intelligence between cybersecurity vendors discussed in this research is yet another example. In recent years, many security vendors embraced the use of CTI as a defense concept,

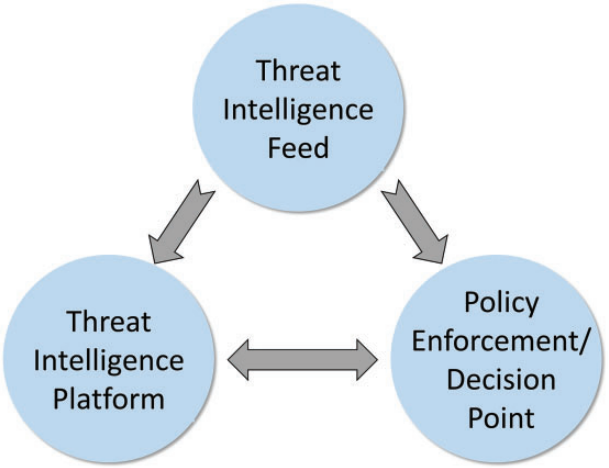


**Figure 1:** Disaggregated components of a threat intelligence solution. The source point of this information flow is a threat intelligence feed, and the destination is a decision or enforcement point. An optional Threat Intelligence Platform (TIP) can act as an exchange/aggregation point between several feeds and multiple enforcement or decision points.

providing their customers with a viable threat intelligence feed solution. In the past, threat sharing in the security vendor space was implemented within the vendor's boundaries. In this legacy model, end customers implicitly shared threats and intelligence with other customers of the same vendor as the products deployed in their premises were connected to the same centralized cloud-based repository. Currently, the adoption of standards and advancements in open Application Programming Interfaces (APIs) allow the disaggregation of CTI solution components. Vendors can mutually use feeds from one another and sell or share their knowledge and services directly or through other vendors. As a result, an ecosystem of solutions for threat data collection, analysis, and collaboration is commercially available. The companies involved in this ecosystem are legacy security vendors with policy enforcement or decision-point products,[13] threat-intelligence-focused firms, service providers that offer managed CTI services, and related consulting/training firms.

Figure 1 illustrates an actionable threat intelligence solution, consisting of three disaggregated components that may be delivered by one or several vendors, using single or multiple products, residing on customer premises or in the cloud.

## Network structure

The sum of cooperation relationships between firms in the same industry creates a consolidated view of its network structure. Such collaborations can be studied by means of the social network analysis approach and techniques with actors represented as nodes in the network and information exchange relationships as the connections between them [33]. As opposed to a randomly generated network, such a representation generates a complex, real-world network with topological and structural properties that are not driven by randomness. There is an increasing interest in studying the underlying organizational principles of complex networks and in identifying

9 As described in the Trusted Automated eXchange of Indicator Information (TAXII™) standard: http://taxiiproject.github.io/about/

10 The Financial Services Information Sharing and Analysis Center: https://www.fsisac.com/

11 Facebook's ThreatExchange initiative (https://threatexchange.fb.com/).

12 Cyber Information Sharing and Collaboration Program (CISCP): https://www.dhs.gov/ciscp

13 A decision point is a network device or software on which policy decisions are made, whereas an enforcement point is where those policies are carried out and enforced. Often, these two functions are integrated into a single product or solution.

common characteristics. Three of these properties, namely, average path length, clustering coefficient, and degree distribution, play key roles in the study and development of complex network theory [34].

A network characterized by high clustering and short path length is called a small-world network. This network exhibits a structure in which most nodes can be reached from every other node by a small number of hops, although they are not directly connected; this is best described by the expression "six degrees of separation".[14] A small-world network is the most efficient and equitable structure for effective knowledge diffusion [35]. Consequently, a significant number of information-sharing-related empirical papers demonstrate small-worldness [14, 15, 18–20]. In the context of the researched domain, such a network would be optimal for threat intelligence sharing, as the importance for near real-time delivery of CTI objects is on the rise.

The third meaningful network property mentioned above, namely, degree distribution, often indicates a scale-free structure, which demonstrates the preferential link attachment phenomenon of the "rich-gets-richer" [36]. However, it will not be further analyzed in this article and could be considered for a follow-up study.

Small-world networks are often associated with the presence of community structure [15]. Community structure reflects the division of network nodes into groups within which the network connections are dense, but between which they are sparser [37]. The subsets of nodes that are densely connected internally are also known as clusters and are best described by the phrase "the friends of my friends are also my friends". Von Hippel [38] suggested that a profitable business approach manifesting communities would be to form coalitions and restrict them to only a subset of firms in the industry. This motivation is in line with the business strategy suggested by Brandenburger and Nalebuff [17] to increase the combined added value of the cooperating firms against the competition.

In accordance with these sources, we propose the following:

**Theory 1: The threat-intelligence-sharing network between cybersecurity vendors is divided into communities and exhibits a small-world structure.**

### Coopetition

Collaboration between competing firms is increasingly capturing scholars' attention due to its growing relevance to business practices [26, 39, 40]. Brandenburger and Nalebuff [17] named this phenomenon coopetition. They developed a related business model and framework that draw on the insights of game theory and suggested using it as a strategy for companies to create and capture value. Other researchers concur that this strategy could yield performance benefits for the participating firms [27, 29, 41, 42].

As cited in Gnyawali and Park [39], Harbison and Pekar, Jr found that over 50% of collaborative relations (strategic alliances) between firms occur among competitors within the same industry. In addition, Bleeke and Ernst [21] indicated that complementary skills and capabilities of two cooperating companies are significant factors supporting collaboration success. Similarly, Von Hippel [22] suggested that collaboration for knowledge sharing among competitors occurs when the combined knowledge yields better results than individual knowledge, implying that complementary capabilities might increase the value of the outcome. Furthermore, in the context of the domain under discussion, R&D-based technology collaborations seem to be a similar type of cooperation. Hagedoorn [43] performed empirical research of R&D networks across different sectors and suggested that those alliances are associated with technological complementarity and noncore fields.

In accordance with these sources, we suggest the following:

**Theory 2: The threat-intelligence-sharing relationships between cybersecurity vendors represent coopetition between complementary solutions.**

### Information sharing

The literature implies that there is an association between the level of information sharing and a firm's success. Gordon *et al*. [11] analyzed the trade-off between information security investments and sharing cyber information and argue that sharing companies spend less money on security systems to reach the same level of protection attained by companies that do not share. A more recent game theoretic framework presented by Tosh *et al*. [12] investigates the economic benefits of cyber-threat information sharing and analyzes the impacts and consequences of not participating in this non-cooperative game. They followed with an incentive model to foster the firm's sharing behavior and maximize its gross utility and found that firms are more incentivized when they share more information among one another. Schrader [44] offered evidence for a positive link between the economic performance of a firm and the participation of its employees in informal information trading.

In related empirical works, Gay and Dousset [25] demonstrated a positive correlation between network centrality and firm innovation capability in the biotechnology sector, and Fershtman and Gandal [24] discovered an association between an open-source project's centrality and its real-world success (measured by the number of times it was downloaded). Gnyawali and Park [26] suggested that firms with prospecting strategies, which strive to be the first mover or close follower in their industry, are likely to look for more coopetition opportunities. Coopetition could help the partnering companies overcome major technological challenges, advance technological innovation, and create other benefits [39].

Based on these sources, we propose the following:

**Theory 3: Structural features of firms in the cybersecurity threat-intelligence-sharing network are associated with real-world success.**

## Research essentials

### Dataset sources and coding

The dataset for this empirical study was uniquely coded from public sources of information and contains two types of records: company and relationship. Figure 2 visualizes the sources used to construct both the vendor and relationship datasets and lists some of the coded attributes.

The company record includes the reference list of vendors in the Cybersecurity500[15] report, which ranks the world's hottest and most innovative companies in the cybersecurity industry based on the selection criteria described in Table A1. In addition to CS500

14 A theory, originally proposed in 1929 by the Hungarian writer Frigyes Karinthy, which connects anyone on the planet to any other person by a chain of no more than five people and six steps.

15 The Cybersecurity500 list (CS500) is compiled by Cybersecurity Ventures on a quarterly basis. The analysis was performed with the Q1/2016 rankings collected from: https://cybersecurityventures.com/cybersecurity-500-list/

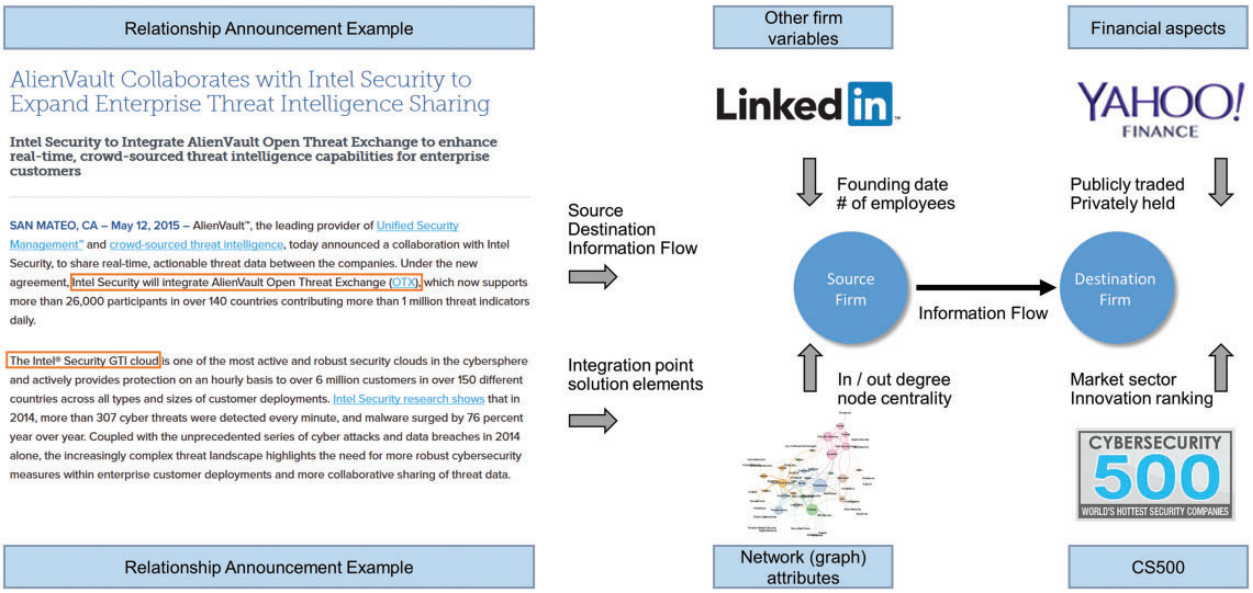


**Figure 2:** Visualization of dataset coding for company and relationship records. The source and destination firms of each CTI relationship were extracted from a public announcement. Company-related attributes were taken from CS500, LinkedIn, and Yahoo! Finance. Graph properties per vendor are based on the network structure formed between the firms.

properties, the record lists informative details such as foundation year and size, the market categories in which the firm operates, and graph properties such as in/out-degree and clustering coefficient. The latter were added based on the network structure formed between the firms. Table A2 summarizes the vendor record fields and their respective sources.

The relationship record structure, detailed in Table A3, is based on press releases, solution briefs, and other publications of threat information sharing established during 2013–16 (Q1). Apart from CTI sharing, no other form of technological cooperation or business alignment was considered, and only relationships in which both companies appear in the CS500 list were included. Each relationship record was manually coded to include the direction of the information flow, the solution elements involved [threat feed, enforcement/decision point, or Threat Intelligence Platform (TIP)], and the technological integration effort used for sharing. Additional fields calculated from these variables include high or low coopetition level (based on the solution element overlap), and four degrees of cooperation intensity (based on the technological integration effort). The latter intensity attribute is visible as an edge weighted degree in the network graph.

The combined coded dataset was expressed as a network of nodes (vertices) connected by links (edges) and visualized as a directed graph. The nodes represent the analyzed list of cybersecurity vendors and the edges are the documented threat-information-sharing relationships between them. All mapped relationships were established directly between two firms, apart from the Cyber Threat Alliance (CTA)[16], which was announced as a group initiative between five vendors. As suggested by Fershtman and Gandal [24], to maintain a unified network view, the two-mode topology of this alliance was projected as a one-mode network with direct connections between all of its members. Once the graph was generated, structure attributes that are often used for social network analysis (SNA) were extracted and added to the company dataset record for further analysis. The formed network includes 57 sharing vendors/nodes out of the 500 nodes in the reference list and 131 sharing relationships/edges connecting them together.

The collection and coding of the dataset have several limitations. First, only publicly announced threat-sharing relationships were considered. Based on the continuous stream of announcements, it is assumed, however, that firms publish their relationships to gain credibility and increase marketing coverage. Second, understanding and coding of the exact nature of each relationship is somewhat subjective and based on the market and industry understanding of the coder. Finally, the rank of each firm and its market category affiliation are based on the subjective analysis of Cybersecurity Venture's analysts.

## Methodology and tools

The article is based on the use of the deductive-reasoning top-down research approach as described by Pawlinski *et al.* [6] and incorporates the relevant theoretical constructs of network structure, coopetition, and information sharing into the threat-intelligence-sharing landscape. Relevant theories were extracted from the existing literature, transformed into hypotheses, and tested against observations derived from the dataset. The observations are discussed in the context of the problem domain to form conclusions. The examination relied on the application of a combination of network (graph) and statistical analysis methods on three distinctive but complementary analysis levels: industry, relationship, and firm, as shown in Table 1.

The chosen research methodology is supported by insights from Haythornthwaite [33], who found two main analysis approaches to networks. The first uses an egocentric network view from a single actor (firm) perspective. The second is based on a complete set of the entities and relationships of the examined environment, which is referred to as the whole-network view. Galaskiewicz and Wasserman, as cited in Provan *et al.* [45], referred to these approaches as micro-level versus macro-level network focuses. In addition, to better understand the relationship attributes, a distinct dyadic view was coded, and the sum of the insights gained from research at the agent, dyadic, and network levels was used to study the industry's ecosystem and

16 Cyber Threat Alliance (CTA): http://cyberthreatalliance.org/

**Table 1:** Mapping literature constructs to analysis perspective

| # | Literature construct | Academic discipline | Supporting theory | Analysis perspective |
|---|---|---|---|---|
| 1 | Network Structure | Computer Science | Social Network Analysis | Industry (Network) |
| 2 | Coopetition | Business Management | Game Theory | Relationship (Dyadic) |
| 3 | Information Sharing | Economics | Knowledge Spillovers/ Information Exchange | Firm (Agent) |

**Table 2:** Small-worldness calculation

| Graph properties | Analyzed network $G$ | Random network $R$ |
|---|---|---|
| Description | 57 sharing nodes, 131 edges | 57 sharing nodes, 131 edges |
| Clustering coefficient | $Cg = 0.103$ | $Cr = 0.047$ |
| Average path length | $Lg = 3.354$ | $Lr = 2.283$ |
| Results | | |
| Clustering coefficient ratio | $\gamma g = \frac{Cg}{Cr} = \frac{0.103}{0.047} = 2.19$ | |
| Average path-length ratio | $\lambda g = \frac{Lg}{Lr} = \frac{3.354}{2.283} = 1.469$ | |
| Small-worldness if $S > 1$ | $S = \frac{\gamma g}{\lambda g} = \frac{2.19}{1.469} = 1.49$ | |

characteristics. Gephi open-source software for graph and network analysis [46] was used to visualize the network communities and extract relevant graph properties.

Finally, as noted by Provan *et al.* [45], different terminology can be used interchangeably to describe companies, relationships, and networks. Throughout this article, an analyzed organization is referred to as a firm, company, vendor, node, agent, or vertex; a relationship between companies is referred to as an edge, collaboration, dyad, or threat intelligence sharing; and a structured network is referred to as an ecosystem or industry.

## Empirical results

### Industry (Network) analysis

Egocentric or dyadic analysis provides a somewhat limited view of the dataset as a collection of separate nodes connected by two-party relationships. In contrast to this view, this section's perspective is focused on the unified structure of the threat-intelligence-sharing ecosystem. The projection of the vendors and their respective relationships into a graph creates a real-world complex network (i.e., a network whose structure is irregular, complex, and dynamically evolving over time) [47]. Measuring basic properties of a complex network, such as its average path length, clustering coefficient, and degree distribution, is a key step toward understanding its structure [34]. These properties are often used in empirical papers, which are categorized as either inter-organizational network analysis or social network analysis studies [14, 15, 24, 45]. Table A4 lists the network properties extracted from the graph created between the sharing vendors, discounting vendors without an active threat intelligence relationship.

A key network property that can be derived from these metrics is small-worldness, which is characterized by high clustering and short path length [48]. The clustering coefficient of a node is the degree to which the firm's edges are connected with each other, and the clustering coefficient of the graph is the average of this value over all nodes. The average path length of a graph is the average number of steps separating two randomly chosen nodes. In accordance with Theory 1, we assume the following:

**Hypothesis 1.1: The cybersecurity threat intelligence network exhibits small-world properties.**

Small-worldness can be quantified by comparing the global clustering coefficient ($C$) and average path length ($L$) of a given network $G$ to an equivalent random network $R$ with the same numbers of nodes and edges. As defined by Watts and Strogatz [49], a network $G$ is said to be a small-world network if $Lg \geq Lr$ and $Cg \gg Cr$. We use the value $S$ to quantify a continuous measure of small-worldness as defined by Humphries and Gurney [48], based on the following tradeoff between high local clustering and short path length: a network is deemed a small-world network if $S > 1$, where $S = \frac{\gamma g}{\lambda g}$, $\gamma g = \frac{Cg}{Cr}$ and $\lambda g = \frac{Lg}{Lr}$. Table 2 lists the calculations used to determine the network's small-worldness.

Given this result, we state the following observation:

**Observation 1.1: The cybersecurity threat intelligence network is a small-world network.**

To validate this observation, $S$ was recalculated after removing all CTA relationships, which were added to the network as a small-world community. The result reinforces Observation 1.1 by demonstrating $S > 1$ as well.

To achieve the small-world characteristic in a real-world complex network, the nodes would need to be grouped into communities called clusters. Therefore, and in accordance with Theory 1, we assume that the analyzed network structure allows for quick and efficient sharing of information across clusters:

**Hypothesis 1.2: The cybersecurity threat intelligence network exhibits a modular structure associated with communities.**

Figure 3 visualizes the partitioning of the network into five communities (clusters) based on the modularity optimization algorithm of Blondel *et al.* [50], which is better known as the Louvain Method, for community detection. The resulting graph is presented using the Fruchterman–Reingold algorithm, showing similar edge lengths with as few crossings as possible [15]. This visualization illuminates the different roles of firms in the ecosystem, such as hubs with large numbers of links or inter-community brokers, and thus highlights the competitive alignment of the companies.

The modularity measure of this graph, $Q = 0.334$, indicates the strength of the network division into communities [50]. This value is maximal when the chosen network is partitioned perfectly, with all links occurring within a given community and no links occurring between different communities. Since values greater than 0.3 appear to

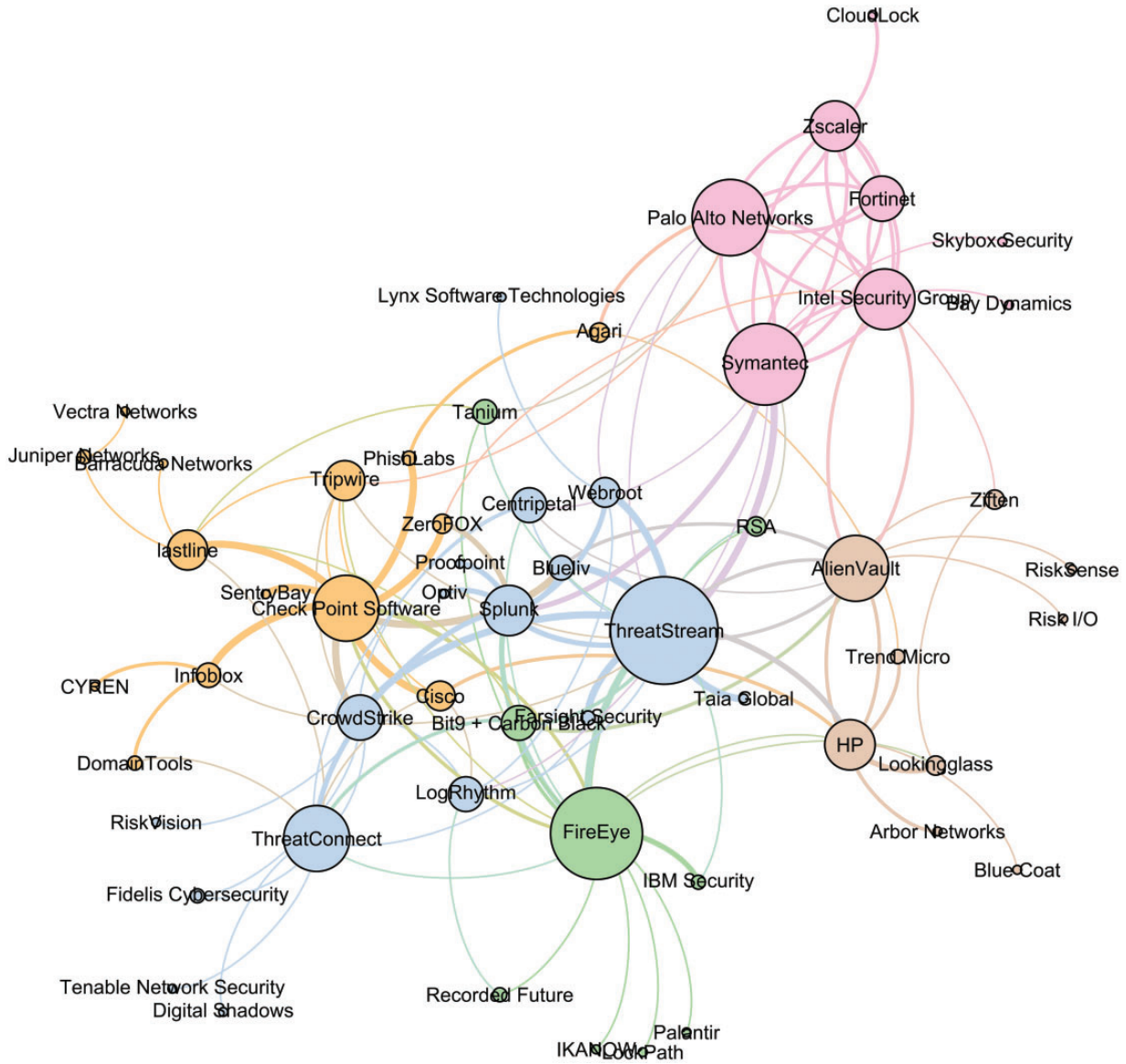


**Figure 3:** Communities formed by threat-intelligence-sharing relationships in the cybersecurity sector. A clockwise curved edge represents an outgoing sharing relationship, and its weight indicates the cooperation intensity of the relationship. Node size corresponds to the total number of relationships (bigger for higher degree), and color indicates the community membership structure.

indicate significant community structure [51], we state the following observation:

**Observation 1.2.1: The cybersecurity threat intelligence network demonstrates a community-related structure.**

To validate this observation, the community structure was recalculated after removing all CTA relationships, which were added to the network as a small-world community, and the result reinforces Observation 1.2.1 by demonstrating a structure of six clusters with a modularity measure of $Q = 0.353$.

To better understand the graph topology and its implications, reachability was further analyzed to determine the connected components in the network [52]. Based on the results, we state the following:

**Observation 1.2.2: The threat intelligence sharing directed network demonstrates a single weakly connected component, a 14-node giant strongly connected component (GSCC), and 43 single-node strongly connected components**[17].

The implications of those findings will be further discussed in the "Discussion and conclusion" section.

## Relationship (dyadic) analysis

Individual firm characteristics and network-level attributes are often used to explain established collaborations. However, there are features that can only be coded when looking at both nodes of each dyad simultaneously. Christakis *et al.* [53] describe the large body of literature that has found links in networks that

17 A strongly connected component is a subgraph with a directed link path from every node to every other node. A weakly connected component is a subgraph with some path from every node to every other node regardless of the link direction. A giant strongly connected component (GSCC) is a strongly connected component that contains a significant fraction of the entire network.

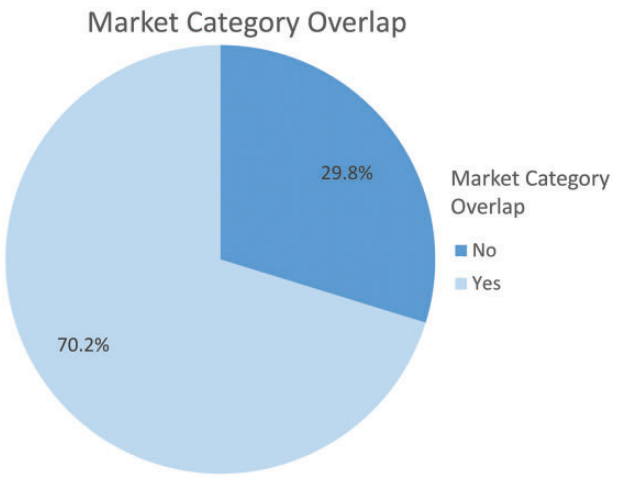


**Figure 4:** Technological market category overlap between vendors in a dyadic relationship.

are associated with correlations in outcomes, thus supporting a dyadic-view analysis approach. The examination in this section was performed per edge using variables derived from the sharing nodes and attributes of the edge itself. The coded dataset consists of several link characteristics, including market category overlap, information flow direction, and relationship strength. Therefore, and in accordance with Theory 2, we suggest the following hypothesis:

**Hypothesis 2.1: The threat intelligence relationships in the cybersecurity sector are formed between vendors that are active in the same market category.**

Inspecting the (one or more) technological market categories of the participating firms in any given relationship, we found that 70.2% of the links are established between vendors that operate in the same category (Fig. 4). To verify the significance of this result, the market category overlap of randomly selected links within the dataset was analyzed, and only 24.4% of the links were established between vendors with overlapping market categories. Therefore, we state the following observation:

**Observation 2.1: Threat-intelligence-sharing relationships in the cybersecurity sector are nearly three times more likely to materialize between competitors.**

Based on the literature, Theory 2 also suggests the relationships are complementary by nature. Therefore, we suggest the following hypothesis:

**Hypothesis 2.2: The threat-intelligence-sharing relationships in the cybersecurity sector are characterized by complementary types of solutions.**

Figure 5 illustrates the intensities of the formed relationships in the network, which are described as suggested by Luo [54] in a diagram of high and low values of competition and cooperation attributes for each relationship. We observed that 72.5% of the relationships are established between complementary solution elements (low competition level), and 79.4% of the relationships demonstrate simple technological integration (low cooperation level). These results are significant when compared to the expected value of 50% for randomly selected links. Therefore, we state the following:

**Observation 2.2: Most of the threat-intelligence-sharing relationships in the cybersecurity sector are loosely integrated and formed between complementary types of solutions.**

## Firm (Agent) analysis

This section considers agent-level (also called egocentric) theories, which are concerned with explaining how the involvement of an organization in a network affects its actions and outcomes [45]. The idea of associating network properties with real-world characteristics was modeled by Meagher and Rogers [20], who showed how the structure of a network of firms influences their aggregate innovativeness. This principle was demonstrated by Fershtman and Gandal [24] and Gay and Dousset [25] in related empirical works. Therefore, and in accordance with Theory 3, we assume the following:

**Hypothesis 3.1: Within the cybersecurity sector, firms with more partnerships are considered more innovative.**

This hypothesis was analyzed by examining the relevant network properties of both the sharing and receiving firms. Spearman's nonparametric correlation was used to determine the relationship between a firm's degree (converted to rank ordering) and a firm's CS500 rank, representing its innovation level and real-world success. Table A5 includes the Spearman correlation coefficient matrix, which indicates a statistically significant positive correlation ($r = 0.22,\ P < 0.01,\ n = 500$) between those variables; consequently, we state the following:

**Observation 3.1: Within the cybersecurity sector, there is a statistically significant positive correlation between the CS500 rank of a firm and its degree.**

As argued by Mascarenhas [27], ownership structure of privately owned versus publicly traded firms results in specific differences in selected dimensions. His empirical research demonstrated that publicly traded firms have a higher rate of growth and suggests that this is a result of better access to credit, market expectations, and management appetite for growth. Therefore, and in accordance with Theory 3, we assume the following:

**Hypothesis 3.2: Within the cybersecurity sector, publicly traded firms participate in threat-intelligence-sharing relationships more than privately held companies.**

As shown in Fig. 6, publicly traded companies participate in threat intelligence sharing more than twice as much as privately held companies[18]. Therefore, we make the following observation:

**Observation 3.2.1: Publicly traded firms are twice as likely to engage in threat-intelligence-sharing relationships.**

As detailed in Table A6 and Table A7, respectively, the effect size is stronger within publicly traded companies ($r = 0.439,\ P < 0.01,\ n = 87$) compared to privately held firms ($r = 0.15,\ P < 0.01,\ n = 413$); hence we state the following:

**Observation 3.2.2: The effect size of the correlation between the degree and innovation rank of a firm is nearly three times stronger among publicly traded companies than privately held companies.**

18 Of publicly traded companies, 19.5% participate in sharing relationships versus 9.4% of privately held firms.

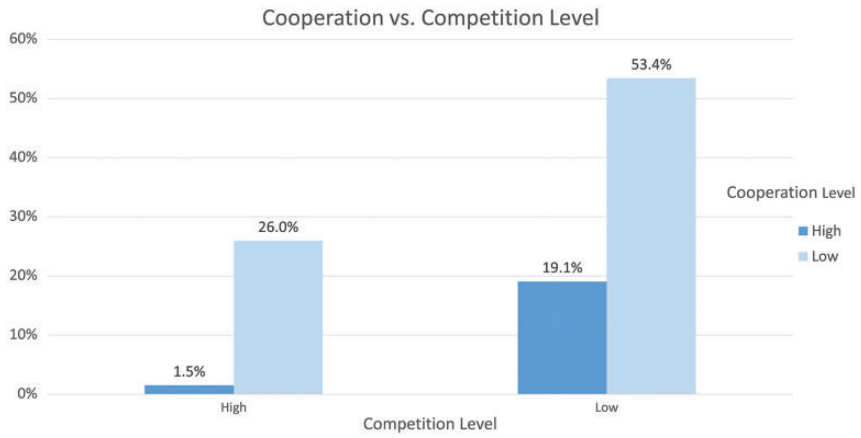


**Figure 5:** Cooperation versus competition in threat intelligence sharing. A sharing relationship between identical solution elements (threat feed, enforcement/decision point, or TIP) is considered highly competitive. A low-cooperation relationship is based on standardized STIX™/TAXII™ or Application Programming Interface (API), while any relationships based on cloud-based sharing or application development are considered highly cooperative.

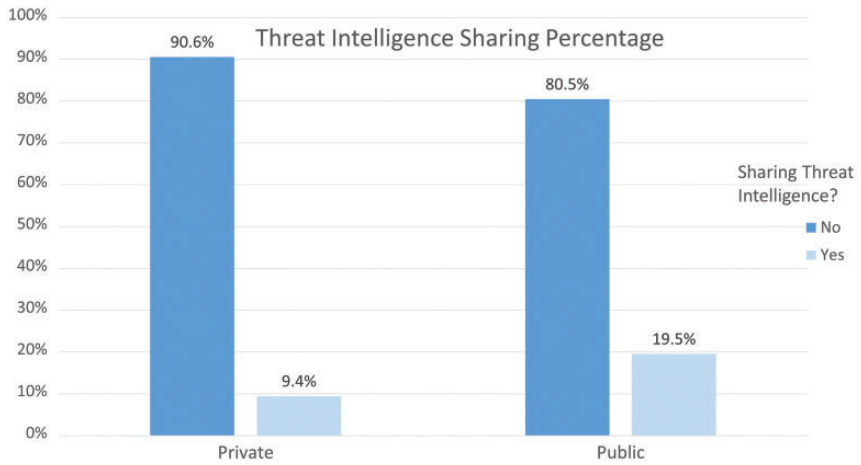


**Figure 6:** Relative sharing percentage of publicly traded versus privately held companies.

## Discussion and conclusion

This section elaborates the research conclusions based on the presented results in light of some notable resources. Further discussion reflects on these conclusions in the problem domain and offers some pragmatic explanations for our findings. Finally, the research contribution and possible limitations are highlighted.

### Network structure

Observation 1.1 reveals that the cybersecurity threat intelligence network exhibits small-world properties, based on the average path length and global clustering coefficient, compared to a similar random network. A small-world network is the most efficient and equitable structure for effective knowledge diffusion [35]. In the context of the researched domain, such a network would be optimal for threat intelligence sharing, as the importance for nearly real-time delivery of CTI objects is on the rise. Also, of interest to the receiving party are the threat intelligence origin and other contextual features that could be possibly deducted from the network structure. However, CTI objects are often described using a family of protocols and languages and already contain this type of contextual data.

A significant amount of information-sharing-related empirical research demonstrates small-worldness in R&D networks [14, 15, 18–20]. The resemblance to the analyzed network in terms of this feature deserves an additional discussion. A key driver for cooperation between companies that are active in the same sector is the potential savings on their R&D expenditures [26]. However, cost reduction might not be the reason for collaboration in the analyzed network, since the established threat-sharing relationships are not R&D collaborations per se but rather facilitate information exchange with relatively low investment. This characteristic implies that there could be other reasons for the cooperation in this market, and these could include technological (better security coverage), commercial (increased credibility and marketing exposure), social (the greater good), and/or not-yet-identified reasons.

A possible explanation for collaboration in the absence of high R&D costs is that for many of the vendors, threat intelligence is not considered a true core business. Either they have other commercially significant product lines or they consume other party feeds as a complementary solution to their primary cyber-related offerings. In addition, market statistics show the lack of a significant revenue stream generated by threat intelligence. Although threat intelligence is growing faster annually than other cybersecurity fields, this market has developed only in the past few years, and it still constitutes a small part of the total cybersecurity expenditure: Its share is expected to reach $1.8B[19] out of $170B in overall global spending

on IT security in 2020.[20] These observations are supported by Hagedoorn [43] who claim that R&D activities in areas close to the firm's core business are not desirable subjects for collaboration and, therefore, cooperation is expected around non-core fields.

The network demonstrates a community-related structure that is divided into five visible clusters, as confirmed in Observation 1.2.1. By looking at the community structure visualization in Fig. 3, one can identify the central hubs of the network based on size and relative location. These are nodes with high degrees of connections that often serve as the boundaries between the formed communities, and the majority of shortest paths pass through them [47]. From an industry perspective, intra-community intelligence sharing can commoditize the threat coverage level and focus the differentiation between the participating vendors within the cluster on other product aspects. As a result, the community members may try to increase their combined market share by leveraging their relationships at the expense of non-sharing vendors; non-sharing vendors are forced to invest more technological and marketing efforts in this field. This explanation is in line with the "changing the game" business strategy suggested by Brandenburger and Nalebuff [17] to increase the combined added value of the cooperating firms against the competition. Von Hippel [38] findings also support this strategy and suggest that a profitable business approach under some conditions would be to form coalitions and restrict them to only a subset of firms in the industry.

Threat intelligence sharing existed as an informal information trading exchange between employees working for different, sometimes directly competing, firms. This phenomenon, known as knowledge spillovers, evolved over time into announced official relationships, although informal exchange presumably still occurs to a certain degree. Unlike computer viruses or disease outbreaks, the mere existence of threat intelligence flow from company A to company B and from company B to company C does not necessarily mean the entire feed of company A is shared with company C. However, as suggested by Fershtman and Gandal [24], direct or indirect knowledge spillovers facilitate the transfer of knowledge and ideas between firms, researchers, and R&D teams, so some threat intelligence might flow from company A to company C even though they are not directly connected.

Given this understanding, we further characterized the network connectivity structure by mapping the connected components. The results are summarized in Observation 1.2.2, and presented in Fig. 7 as a bow tie diagram. About one-third of the companies feed GSCC members with intelligence, and 42% receive it from GSCC members. Assuming knowledge spillovers occur, and in accordance with Newman *et al*. [16], a possible use of this insight would be to identify nodes within the GSCC community that are key to distribution of intelligence. To stop a spread of poisoned intelligence, or to facilitate a rapid delivery of critical intelligence for mitigation, one should focus attention on GSCC nodes in decreasing out-degree order.

Based on this discussion, we form the following conclusion:

**Conclusion 1: The cybersecurity industry exhibits a small-world structure associated with communities, suitable for effective intelligence sharing.**

## Coopetition

Observation 2.1 indicates that threat-intelligence-sharing relationships in the cybersecurity sector are nearly three times more likely to materialize between competing vendors active in the same market category than those of different categories. Therefore, those relationships should be referred to as coopetition. From a market perspective, two factors make the threat-intelligence-sharing ecosystem a coopetition-based environment. The first factor is its high product sustainability characteristic, as demonstrated by the disaggregated components in Fig. 1. Each of these components can be replaced by another vendor's product to construct a viable solution. According to Gal-Or and Ghose [13], sharing is more valuable when product substitutability is higher, implying that such sharing alliances yield greater benefits in more competitive industries. The second factor is based on the concept that short product lifecycle and time-to-market constraints are drivers of cooperation [55]. The threat intelligence market has both features, since threat objects become less relevant as time passes (product lifecycle) and the demand for real-time information to fight the cyber war grows (time to market). The need for near real-time delivery is illustrated by the findings of Verizon Enterprise [56]: 75% of attacks spread from the first victim to the next one within 24 hours, and over 40% hit the second organization in less than an hour. Furthermore, the shared objects have a somewhat limited value based on their short life expectancy, the level of trust required to use them without risking errors, and the need to merge them with other contextual signals to produce uniquely identifiable intelligence. This point is supported by a two-party model that infers information trading is advantageous as long as the information offers "little competitive advantage" [38].

In addition, Observation 2.2 indicates that the dyads are mostly formed between loosely integrated complementary types of solution elements. There are few supporting arguments that explain these findings. A statistical analysis shows that within open-source threat intelligence feeds, object overlap of IOCs was less than 3% [56]. Projecting these results to the threat-sharing ecosystem between vendors, one can assume a low data overlap between them, which can justify aggregating feeds from different vendors. Additionally, Von Hippel [22] suggested that combined knowledge yields better results than individual knowledge, just as combining feeds from different sources might yield better security coverage. Lastly, a model proposed by Hausken [57] indicates that the level of security sharing between two firms increases when the interdependency between the parties grows. This behavior is seen with cybersecurity vendors that utilize each other's research capabilities to increase their overall threat coverage with each firm benefiting from the other's security investments.

Initially, a threat intelligence solution could be based on quantity and diversity by freeriding public open-source CTI feeds without reciprocal sharing. However, to significantly grow a customer base, a wider, contextual-based perspective of the threat landscape is required, and feed attributes such as relevancy and quality must also be considered. This argument is supported by Combs and Ketchen Jr [41], who claimed that growth-minded firms engage in interfirm cooperation to overcome resource constraints to growth. Their viewpoint is grounded in the resource-based view (RBV) strategy described by Barney [23], which is a means to generate a sustained competitive advantage. In the context of the researched domain, access to the resource of uniquely identifiable intelligence can only be achieved with customer-base growth, which facilitates a broader attack landscape perspective. However, the customer base cannot grow unless the company provides real-world, high-quality threat

19 IDC's market analysis: "Worldwide Threat Intelligence Security Services Forecast, 2016-2020: strength in numbers".

20 As quoted in Forbes from research published by MarketsandMarkets: https://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/

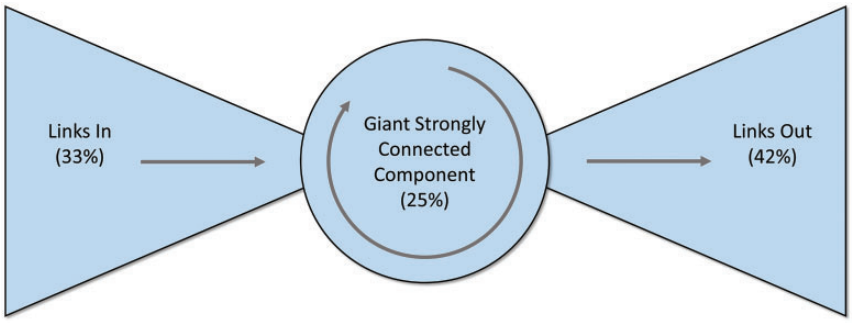


**Figure 7:** The structure and relative component sizes of the threat-intelligence-sharing network.

intelligence. Therefore, sharing CTI between security vendors becomes the means to overcome this catch-22 scenario and could partially explain why sharing companies are ranked higher for innovation and success (Conclusion 3).

As the focus on the accuracy, efficacy, and deployment time of threat intelligence is on the rise, vendors need to increase their investments in this field. Delivering a sustainable CTI solution can be viewed as an opportunity to differentiate or as a burden forcing the vendor to devote increasing amounts of resources in a never-ending arms race against the attackers and the competition. Therefore, companies need to decide whether to cooperate or compete in this domain based on their core focus and product strategy.

Based on this discussion, we form the following conclusion:

**Conclusion 2: The cybersecurity threat-intelligence-sharing relationships are characterized by coopetition between loosely integrated complementary solutions.**

## Information sharing

Observation 3.1 indicates that firms with more threat intelligence partnerships are considered more innovative. This association is supported by Garcia and Velasco [29], who explored the impact of coopetition strategy on business success and found that it contributes positively and significantly to development of product lines and innovative competence. Furthermore, as cited in Morris *et al* [42], Parker argued that firms experiencing high rates of technological change, and firms confronting greater product variety, are likely to pursue cooperative relationships.

While the presence of this correlation does not necessarily suggest causality; it does imply that both degree and innovation rank variables change in the same direction to a certain strength. In this study, we did not determine whether the analyzed correlation is spuriously caused by the presence of a third unseen factor, nor did we determine the order in which the changes happen. Nevertheless, exploring the relationship among these variables is a significant finding as widely discussed in correlational research related literature [58] and demonstrated in similar empirical studies [41, 44].

Scholars claim that ownership structure results in specific differences in selected dimensions [27]. Based on this argument a separate view for publicly traded and privately held firms was created, and the degree to innovation rank association was calculated separately. The results indicate that publicly traded companies participate in threat intelligence sharing twice as much as privately held companies (Observation 3.2.1). We use the correlation coefficient as a key index of effect size and interpret it using Cohen's guidelines as cited in Hemphill [59].[21] The outcome reveals that publicly traded firms demonstrate medium-to-large effect size nearly three times stronger than that of privately held companies with small effect size (Observation 3.2.2). These results are in line with empirical findings showing that publicly traded firms have a higher rate of growth than privately held firms [27] and with models suggesting firms with prospecting growth strategies are more likely to engage in coopetition [26]. Acharya and Xu [28] found that public firms with internal cash flow lower than their investments spend more on R&D and generate a better patent portfolio than their private counterparts; hence they are more innovative. In addition, collaboration among large competing companies was found to yield the biggest positive effect on technological diversity [29]. The latter point could explain, in part, the higher rates of cooperation among publicly traded firms that tend to be larger than privately held companies.

Given the growing number of threat-sharing relationships that have been announced since the dataset was constructed,[22] it appears that vendors acknowledge the added value in taking part in this ecosystem. A significant difference related to information exchange between the cybersecurity sector and other verticals facilitates this decision. The relationships in this study are mostly established directly between two firms,[23] whereas in most other verticals the threat intelligence exchange is facilitated by a central trusted entity that acts as a clearing center and removes any sensitive data from the flow. The hub-and-spoke-based central processing structure demonstrated in other verticals has led Liu, Zafar and Au [8] and Tosh *et al*. [12] to identify a critical incentive-alignment issue in threat information sharing. In the absence of appropriate controls, firms might attempt to free ride on the security expenditures of others. This problem does not exist in the ecosystem under discussion where the shared information value is readily evaluated by the receiving party.[24]

Based on this discussion, we form the following conclusion:

**Conclusion 3: The number of threat-sharing relationships of a firm is positively associated with its innovation level; the effect size is nearly three times stronger among publicly traded companies than privately held companies.**

21 Correlation coefficients in the order of 0.10 are "small," those of 0.30 are "medium," and those of 0.50 are "large" in terms of magnitude of effect sizes.

22 Recent examples include Checkpoint which joined the CTA alliance in February 2017 and the Cisco-IBM cooperation revealed in May 2017.

23 The relationships mapped in this study were all direct with the exception of CTA.

24 To discourage free riders, the Cyber Threat Alliance has defined measurable contributions expected from any security vendor that joins the alliance.

**Table 3**: Summary of theories, hypotheses, observations, and conclusions

| Literature Construct | Theory | Hypotheses | Observations | Conclusion |
|---|---|---|---|---|
| Network Structure | Theory 1: The threat-intelligence-sharing network between cybersecurity vendors is divided into communities and exhibits a small-world structure. | Hypothesis 1.1: The cybersecurity threat intelligence network exhibits small-world properties.<br>Hypothesis 1.2: The cybersecurity threat intelligence network exhibits a modular structure associated with communities. | Observation 1.1: The cybersecurity threat intelligence network is a small-world network.<br>Observation 1.2.1: The cybersecurity threat intelligence network demonstrates a community-related structure.<br>Observation 1.2.2: The threat intelligence sharing directed network demonstrates a single weakly connected component, a 14-node giant strongly connected component (GSCC), and 43 single-node strongly connected components. | Conclusion 1: The cybersecurity industry exhibits a small-world structure associated with communities, suitable for effective intelligence sharing. |
| Coopetition | Theory 2: The threat-intelligence-sharing relationships between cybersecurity vendors represent coopetition between complementary solutions. | Hypothesis 2.1: The threat intelligence relationships in the cybersecurity sector are formed between vendors that are active in the same market category.<br>Hypothesis 2.2: The threat-intelligence-sharing relationships in the cybersecurity sector are characterized by complementary types of solutions. | Observation 2.1: Threat-intelligence-sharing relationships in the cybersecurity sector are nearly three times more likely to materialize between competitors.<br>Observation 2.2: Most of the threat-intelligence-sharing relationships in the cybersecurity sector are loosely integrated and formed between complementary types of solutions. | Conclusion 2: The cybersecurity threat-intelligence-sharing relationships are characterized by coopetition between loosely integrated complementary solutions. |
| Information Sharing | Theory 3: Structural features of firms in the cybersecurity threat-intelligence-sharing network are associated with real-world success. | Hypothesis 3.1: Within the cybersecurity sector, firms with more partnerships are considered more innovative.<br>Hypothesis 3.2: Within the cybersecurity sector, publicly traded firms participate in threat-intelligence-sharing relationships more than privately held companies. | Observation 3.1: Within the cybersecurity sector, there is a statistically significant positive correlation between the CS500 rank of a firm and its degree.<br>Observation 3.2.1: Publicly traded firms are twice as likely to engage in threat-intelligence-sharing relationships.<br>Observation 3.2.2: The effect size of the correlation between the degree and innovation rank of a firm is nearly three times stronger among publicly traded companies than privately held companies. | Conclusion 3: The number of threat-sharing relationships of a firm is positively associated with its innovation level; the effect size is nearly three times stronger among publicly traded companies than privately held companies. |

## Contribution and limitations

This article aims to make a twofold contribution to research. First, it contributes to domain knowledge by analyzing a novel dataset of a threat-intelligence-sharing ecosystem between cybersecurity vendors, identifying some of its related characteristics and insights, visualizing hubs, brokers, communities, and other patterns in the network structure, and discussing the results in the context of the cybersecurity industry. We know of no other study that has attempted to analyze explicitly the CTI sharing among vendors. Second, this article contributes to methodology by offering a unique breadth of perspectives of the problem domain, mapping multidisciplinary theoretical constructs into the research domain from the network, dyad, and agent views, and studying these perspectives using statistics and graph analysis methods.

Table 3 summarizes the knowledge contributions by listing the relevant theories, formed hypotheses and their associated observations, and the derived conclusions of this study.

The insights and discussion presented in this study are increasingly relevant, given the growing market traction of threat intelligence sharing and the constantly evolving nature of the analyzed ecosystem. The findings will be of use to policy decision makers in all sectors as sharing strategies are considered and to regulation authorities as they encourage threat information exchange within verticals. These results can also be utilized by security vendors to assess their firm's relative location and competitive position within the threat-intelligence-sharing ecosystem. The reference list of implications and lessons suggested by Iyer *et al*. [14] can facilitate examination of the network visualization and development of a scorecard

to help an individual firm leverage its network position for competitive advantage. Moreover, although the empirical setting of this paper is the cybersecurity sector, the multidisciplinary research methodology and lessons can be generalized and adapted to other sharing initiatives and domains.

The study could become a baseline for further research in the same problem domain. Follow-up directions will likely fall into two areas. The first is analysis of the industry perspective over time including studies of how the network evolves, how node characteristics change, how the knowledge diffuses between vendors, and how dyadic relationships are formed and severed. Whereas small-world characteristics found in the ecosystem define the network structure, they do not explain why the network was formed with a particular structure [60], so the link selection criteria and exact sharing motivations are yet to be studied. The second direction for follow-up will involve the agent-view analysis of internal and external forces influencing sharing decisions by vendors. This perspective is grounded in the Value Net schematic map of Brandenburger and Nalebuff [17], which describes the different market players, such as customers and competitors that influence a vendor's coopetitive behavior. Furthermore, comparing the optimal network formed based on individual vendor incentives with the network that maximizes overall societal welfare can reveal disparities and tensions between these approaches as described by Jackson [61] and can identify methods for optimization.

On a final note, despite all efforts, the research has some limitations in methodology and results. First, it includes only a single snapshot in time, and the network is dynamically changing with new relationships, company acquisitions, financial results, and innovation rankings. Second, some relevant studies may not have been covered, so the possible hypotheses or discussion points they provoke were missed. Third, only publicly announced threat-sharing relationships between cybersecurity vendors were considered. Lastly, the coding procedures of several variables as well as the Cybersecurity500 ranking are somewhat subjective and depend on the professional views and experience of the coder.

## Funding

This work was supported by the Blavatnik Interdisciplinary Cyber Research Center (ICRC) at Tel Aviv University.

## Acknowledgments

The author is grateful to Ohad Barzilay for insightful discussions, Neil Gandal for continuous guidance, and the journal reviewers whose comments and suggestions have greatly improved the article.

## Appendix

**Table A1:** Cybersecurity 500 ranking selection criteria as listed by Cybersecuirty Ventures.

| Selection criteria | |
|---|---|
| Market category | Company growth |
| Problem(s) solved | Published product reviews |
| Customer base | Demos and presentations at conferences |
| Feedback from CISOs and Decision makers | Corporate marketing and branding |
| Feedback from IT Security Evaluators & Recommenders | Media coverage |
| Feedback from VARs, SIs, and Consultants | Notable implementations |
| VC Funding | Founder and management pedigree |
| | Interviews with senior management |

**Table A2:** Company record structure (500 records)

| Attribute | Source | Attribute | Source |
|---|---|---|---|
| Company name, innovation rank, market categories, publicly traded/privately held | CS500, LinkedIn, Yahoo! Finance | In-degree and out-degree of sharing relationships | Network graph[b] |
| Location, no. of employees, founding date[a] | CS500, LinkedIn, Yahoo! Finance | Other graph metrics (clustering coefficient, Betweenness Centrality)[a] | Network graph[b] |

[a]Attributes that can be used in future research.
[b]Calculated using Gephi from the structure of nodes (companies) and edges (relationships).

**Table A3:** Relationship record structure (131 records involving 57 companies)

| Attribute | Source | Attribute | Source |
|---|---|---|---|
| Sharing/receiving parties | Direction of relationship coded from press release/ white paper | Cooperation level (High/Low) | The integration effort coded from the press release/white paper |
| Competition level (High/Low) | Overlap of solution elements involved[a] coded from the press release/ white paper | Market category overlap (Yes/No) | A firm's market categories as described in the CS500 list |

[a]As described in Fig. 1

**Table A4**: Key network metrics

| Graph metric | Value | Graph Metric | Value |
|---|---|---|---|
| Graph type | Directed | Graph Density (Directed) | 0.041 |
| Vertices | 57 | Average Clustering Coefficient | 0.103 |
| Total edges | 131 | Average Path Length | 3.354 |

**Table A5**: Degree to rank Spearman correlation (all firms)

| Spearman's rho | | CS500 Rank | Degree (Ranked) |
|---|---|---|---|
| CS500 Rank | Correlation Coefficient | 1.000 | −0.220[b] |
| | Significance (two-tailed) | | 0.000[a] |
| | N | 500 | 500 |
| Degree (Ranked) | Correlation Coefficient | −0.220[b] | 1.000 |
| | Significance (two-tailed) | 0.000[a] | |
| | N | 500 | 500 |

[a]Correlation is significant at the 0.01 level (two-tailed).

[b]Negative values indicate a positive correlation since lower CS500 rank is better.

**Table A6**: Degree to rank Spearman correlation (publicly traded firms only)

| Spearman's rho | | CS500 Rank | Degree (Ranked) |
|---|---|---|---|
| CS500 Rank | Correlation coefficient | 1 | −0.439[b] |
| | Significance (two-tailed) | | 0.000[a] |
| | *N* | 87 | 87 |
| Degree (Ranked) | pearson correlation | −0.439[b] | 1 |
| | Significance (two-tailed) | 0.000[a] | |
| | *N* | 87 | 87 |

[a]Correlation is significant at the 0.01 level (two-tailed).

[b]Negative values indicate a positive correlation since lower CS500 rank is better.

**Table A7**: Degree to rank Spearman correlation (privately held firms only)

| Spearman's rho | | CS500 Rank | Degree (Ranked) |
|---|---|---|---|
| CS500 Rank | Correlation coefficient | 1 | −0.150[b] |
| | Significance (two-tailed) | | 0.002[a] |
| | *N* | 413 | 413 |
| Degree (Ranked) | Pearson correlation | −0.150[b] | 1 |
| | Significance (two-tailed) | 0.002[a] | |
| | *N* | 413 | 413 |

[a]Correlation is significant at the 0.01 level (two-tailed).

[b]Negative values indicate a positive correlation since lower CS500 rank is better.

## References


1. Ablon L, Libicki MC, Golay AA. *Markets for Cybercrime Tools and Stolen Data: Hackers*' Bazaar. Santa Monica, CA: Rand Corporation, 2014.
2. Burger EW, Goodman MD, Kampanakis P. *Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies. Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*: ACM, 2014, 51–60.
3. Qamar S, Anwar Z, Rahman MA, *et al*. Data-driven analytics for cyber-threat intelligence and information sharing. *Comp Sec* 2017; **67**:35–58.
4. Fransen F, Smulders A, Kerkdijk R. Cyber security information exchange to gain insight into the effects of cyber threats and incidents. *E & I Elektrotech Inform* 2015; **132**:106–112.
5. Krishnan R, Sandhu R, Ranganathan K. PEI Models towards Scalable, Usable and High-Assurance Information Sharing. *Proceedings of the 12th ACM symposium on Access control models and technologies*: ACM, 2007, 145–50.
6. Pawlinski P, Jaroszewski P, Urbanowicz J, *et al*.; Standards and Tools for Exchange and Processing of Actionable Information. *European Union Agency for Network and Information Security, Heraklion, Greece* 2014.
7. Zhao W, White G; A collaborative information sharing framework for community cyber security. *Homeland Security (HST), 2012 IEEE Conference on Technologies for*: IEEE, 2012, 457–62.
8. Liu CZ, Zafar H, Au YA. Rethinking fs-isac: an it security information sharing network model for the financial services sector. *Comm Assoc Inform Syst* 2014; **34**:2.
9. Ring T. Threat intelligence: why people don't share. *Comp Fraud Sec* 2014; **2014**:5–9.
10. Zrahia A. A multidisciplinary analysis of cyber information sharing. *Military Strat Affairs* 2014; **6**:59–77.
11. Gordon LA, Loeb MP, Lucyshyn W. Sharing information on computer systems security: an economic analysis. *J Acc Public Pol* 2003; **22**:461–85.
12. Tosh DK, Sengupta S, Mukhopadhyay S, *et al*. ; *Game Theoretic Modeling to Enforce Security Information Sharing among Firms. Cyber Security and Cloud Computing (CSCloud), 2015 IEEE 2nd International Conference on*: IEEE, 2015, 7–12.
13. Gal-Or E, Ghose A. The economic incentives for sharing security information. *Inform Syst Res* 2005; **16**:186–208.
14. Iyer B, Lee C-H, Venkatraman N. Managing in a "small world ecosystem": lessons from the software sector. *California Manage Rev* 2006; **48**:28–47.
15. Tomasello MV, Napoletano M, Garas A, *et al*. The rise and fall of R&D networks. *arXiv Preprint arXiv* 2013;**1304**:3623.
16. Newman ME, Forrest S, Balthrop J. Email networks and the spread of computer viruses. *Phys Rev E* 2002; **66**:035101.
17. Brandenburger AM, Nalebuff BJ. The right game: use game theory to shape strategy. *Harvard Business Rev* 1995; **73**:57–71.
18. Hagedoorn J. Inter-firm R&D partnerships: an overview of major trends and patterns since 1960. *Res Pol* 2002; **31**:477–92.
19. Hanaki N, Nakajima R, Ogura Y. The dynamics of R&D network in the IT industry. *Res Pol* 2010; **39**:386–99.
20. Meagher K, Rogers M. Network density and R&D spillovers. *J Econ Behav Org* 2004; **53**:237–60.
21. Bleeke J, Ernst D. The way to win in cross-border alliances. *Harvard Business Rev* 1991; **69**:127–35.
22. Von Hippel E. *Cooperation between Rivals: Informal Know-How Trading*. Dordrecht: Springer, 1989, 157–175.
23. Barney J. Firm resources and sustained competitive advantage. *J Manag* 1991; **17**:99–120.
24. Fershtman C, Gandal N. Knowledge spillovers: the "social network" of open-source projects. *RAND J Econ* 2011; **42**:70–91.
25. Gay B, Dousset B. Innovation and network structural dynamics: study of the alliance network of a major sector of the biotechnology industry. *Res Pol* 2005; **34**:1457–75.
26. Gnyawali DR, Park BJR. Co-opetition and technological innovation in small and medium-sized enterprises: a multilevel conceptual model. *J Small Business Manage* 2009; **47**:308–30.
27. Mascarenhas B. Domains of state-owned, privately held, and publicly traded firms in international competition. *Admin Sci Quart* 1989; **34**: 582–97.
28. Acharya V, Xu Z. Financial dependence and innovation: the case of public versus private firms. *J Fin Econ* 2017; **124**:223–243.
29. Garcia CQ, Velasco CA. *Co-opetition and performance: evidence from European biotechnology industry. II Annual Conference of EURAM on "Innovative Research Management"*, Stockholm: Citeseer, 2002.
30. Chismon D, Ruks M. *Threat Intelligence: Collecting, Analysing, Evaluating*. Basingstoke, UK: MWR InfoSecurity Ltd, 2015.
31. Harrison K, White G. Information sharing requirements and framework needed for community cyber incident detection and response. *Homeland Security (HST), 2012 IEEE Conference on Technologies for*: IEEE, 2012, 463–9.

32. Johnson C, Badger L, Waltermire D, *et al*. Guide to cyber threat information sharing. *NIST Special Publication*, 2016; **800**:150.
33. Haythornthwaite C. Social network analysis: an approach and technique for the study of information exchange. *Lib Inform Sci Res* 1996; **18**:323–342.
34. Wang XF, Chen G. Complex networks: small-world, scale-free and beyond. *Circuits Syst Mag, IEEE* 2003; **3**:6–20.
35. Kim H, Park Y. Structural effects of R&D collaboration network on knowledge diffusion performance. *Exp Syst Appl* 2009; **36**:8986–92.
36. Barabasi AL, Albert R. Emergence of scaling in random networks. *Science* 1999; **286**:509–512.
37. Newman ME, Girvan M. Finding and evaluating community structure in networks. *Phys Rev E Stat Nonlin Soft Matter Phys* 2004; **69**:026113.
38. Von Hippel E. Cooperation between rivals: informal know-how trading. *Res Pol* 1987; **16**:291–302.
39. Gnyawali DR, Park B-J. Co-opetition between giants: collaboration with competitors for technological innovation. *Res Pol* 2011; **40**:650–63.
40. Ritala P, Golnam A, Wegmann A. Coopetition-based business models: the case of Amazon.com. *Ind Market Manage* 2014; **43**:236–49.
41. Combs JG, Ketchen DJ. Jr Explaining interfirm cooperation and performance: toward a reconciliation of predictions from the resource-based view and organizational economics. *Strat Manage J* 1999; **20**:867–88.
42. Morris MH. Koçak A, Özer A; Coopetition as a small business strategy: implications for performance. *J Small Business Strat* 2007; **18**:35.
43. Hagedoorn J. Understanding the rationale of strategic technology partnering: interorganizational modes of cooperation and sectoral differences. *Strat Manage J* 1993; **14**:371–85.
44. Schrader S. Informal technology transfer between firms: cooperation through information trading. *Res Pol* 1991; **20**:153–70.
45. Provan KG, Fish A, Sydow J. Interorganizational networks at the network level: a review of the empirical literature on whole networks. *J Manage* 2007; **33**:479–516.
46. Bastian M, Heymann S, Jacomy MJI. *Gephi: an Open Source Software for Exploring and Manipulating Networks* 2009. *Icwsm* 2009; **8**:361–362.
47. Boccaletti S, Latora V, Moreno Y, *et al*. Complex networks: structure and dynamics. *Phys Rep* 2006; **424**:175–308.
48. Humphries MD, Gurney K. Network 'small-world-ness': a quantitative method for determining canonical network equivalence. *PLoS One* 2008; **3**:e0002051.
49. Watts DJ, Strogatz SH. Collective dynamics of 'small-world'networks. *Nature* 1998; **393**:440.
50. Blondel VD, Guillaume J-L, Lambiotte R, *et al*. Fast unfolding of communities in large networks. *J Stat Mech* 2008; **2008**:P10008.
51. Newman ME. Fast algorithm for detecting community structure in networks. *Phys Rev E* 2004; **69**:066133.
52. Tarjan R. Depth-first search and linear graph algorithms. *SIAM J Comp* 1972; **1**:146–60.
53. Christakis NA, Fowler JH, Imbens GW, *et al*. An empirical model for strategic network formation. *National Bureau of Economic Research*, 2010.
54. Luo Y. *Coopetition in International Business*. Copenhagen, Denmark: Copenhagen Business School Press DK, 2004.
55. Gnyawali DR, He J, Madhavan R. Impact of co-opetition on firm competitive behavior: an empirical examination. *J Manage* 2006; **32**: 507–30.
56. Verizon Enterprise RT. 2015 Data Breach Investigations Report. 2015. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf
57. Hausken K. Information sharing among firms and cyber attacks. *J Account Public Pol* 2007; **26**:639–88.
58. Hale J. The importance of correlational studies. *Psych Central* 2011. https://psychcentral.com/blog/the-importance-of-correlational-studies/.
59. Hemphill JF. *Interpreting the Magnitudes of Correlation Coefficients* 2003. *American Psychologist* 2003; **58**:78–79.
60. Jackson MO, Rogers BW. The economics of small worlds. *J Eur Econ Assoc* 2005; **3**:617–627. -3):
61. Jackson MO. *Social and Economic Networks*. Princeton: Princeton University Press, 2008.