Cyber Threat Intelligence Sharing: Survey and Research Directions

Thomas D. Wagner[a,*], Khaled Mahbub[a], Esther Palomar[a], Ali E. Abdallah[a]

[a]*Birmingham City University, Curzon Street, Birmingham, B4 7XG, UK*

Abstract

Cyber Threat Intelligence (CTI) sharing has become a novel weapon in the arsenal of cyber defenders to proactively mitigate increasing cyber attacks. Automating the process of CTI sharing, and even the basic consumption, has raised new challenges for researchers and practitioners. This extensive literature survey explores the current state-of-the-art and approaches different problem areas of interest pertaining to the larger field of sharing cyber threat intelligence. The motivation for this research stems from the recent emergence of sharing cyber threat intelligence and the involved challenges of automating its processes. This work comprises a considerable amount of articles from academic and gray literature, and focuses on technical and non-technical challenges. Moreover, the findings reveal which topics were widely discussed, and hence considered relevant by the authors and cyber threat intelligence sharing communities.

Keywords: advanced persistent threat, cyber threat intelligence, threat sharing, relevance, trust, anonymity, literature survey.

1. Introduction

Cyber Threat Intelligence (CTI) sharing promises to be a new method to create situation awareness among sharing stakeholders [1]. Moreover, it is seen as a necessity to survive current and future attacks by working proactively instead of only reactive. It may become obligatory for organizations to have a threat intelligence program being part of proactive cyber security and share their information. Stakeholders may be held responsible in the future for not sharing known threats that affected others and resulted in a breach. The core idea behind threat intelligence sharing is to create situation awareness among stakeholders through sharing information about the newest threats and vulnerabilities, and to swiftly implement the remedies. Furthermore, CTI can aid stakeholders in making tactical decisions. It is a challenging task for practitioners to implement a CTI program that consumes and disseminates the information in a timely fashion. Moreover, stakeholders struggle to

*I am corresponding author

Email addresses: thomas.wagner@bcu.ac.uk (Thomas D. Wagner), khaled.mahbub@bcu.ac.uk (Khaled Mahbub), esther.palomar@bcu.ac.uk (Esther Palomar), ali.abdallah@bcu.ac.uk (Ali E. Abdallah)

implement a system that properly consumes CTI and makes the information relevant. The biggest challenge that most practitioners may face, before sharing their own CTI, is how to make use of information, i.e., how to comprehend the information and implement its remedy. The literature reveals that stakeholders would like to participate in an effective and automated sharing process, but insufficient models and tools render it challenging [2]. Nevertheless, manual sharing is a widely used approach to exchange information about vulnerabilities. I.e., stakeholder to stakeholder sharing where a trusted relationship already exists or sharing through trusted groups such as an Information Sharing and Analysis Center (ISAC)[1]. The goal is to create situation awareness among stakeholders and to be alerted about a threat as quickly as possible. Although, a manual approach to sharing CTI may be ineffective for several reasons. For instance, slow sharing of new threats, human error rate during processing, or subjective relevance filtering. Consequently, automating some of the processes may increase the effectiveness of CTI sharing. CTI sharing occurs on a global scale and every country has different laws and regulations regarding what information attribute is considered private; for example, what can be legally shared and what has to be anonymized. This literature survey focuses on current challenges that may impede the sharing process. Actionability of threat information is discussed by various sources which reflect the following attributes: trust, reputation, relevance, anonymity, timeliness, and data interoperability. Trust is a fundamental pillar of any information sharing program, therefore trusted relationships have to be established before any critical threat intelligence is shared. Governance, management, policies, and legal factors were analyzed that may support or impede CTI sharing. Threat intelligence is mostly shared on a national level but international exchanges are gaining momentum, especially between larger organizations that operate worldwide. Nevertheless, some groups strictly share on a national level, such as the Cyber Security Information Sharing Partnership (CiSP)[2] in the United Kingdom. The human behavior, as well as cultural and language barriers regarding CTI sharing are briefly discussed to emphasize the challenges faced among international stakeholders. Incentives are offered by various authors to encourage stakeholders to participate in a threat sharing model. The major challenge is for organizations to understand how important a CTI sharing program is and will be in the future, and then consequently, invest time and money to build such a program. Due to the relatively recent emerge of CTI sharing and automating its processes, and the resulting limited availability of academic literature, gray literature has therefore been included in the survey.

The rest of the paper is organized as follows: Section 2 generically elaborates on CTI sharing. Section 3 discusses the actionability of CTI. Section 4 presents the regulations. Section 5 provides a summary. Lastly, section 6 concludes our work.

[1]Information Sharing and Analysis Center: https://tinyurl.com/ybxqtk56

[2]Cyber Security Information Sharing Partnership: https://tinyurl.com/h5r6sv5

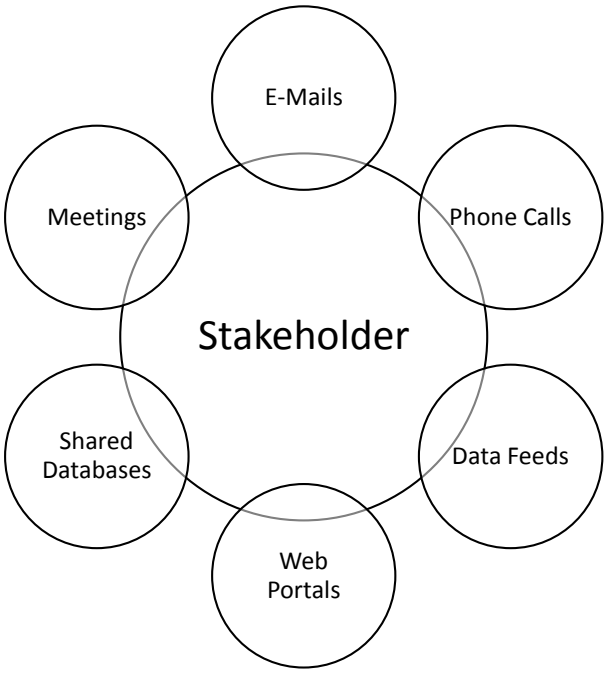

Figure 1: Manual Threat Intelligence Sharing: This figure illustrates various ways of manual CTI sharing.

2. Cyber Threat Intelligence Sharing

In this section we are going to discuss about different aspects of CTI sharing including automation, collaboration, indicators, industry sector sharing, benefits, risks, human role, and cultural and language barriers.

2.1. Automated Sharing of CTI

CTI is not simply information it is information that has been analyzed and is actionable [3]. Current sharing methods are heavily based on manual input and therefore labor intensive. As shown in Figure 1, current CTI sharing is conducted through e-mails, phone calls, web-community portals [4], shared databases, and data feeds [5]. Automation is a necessity to cope with the flood of internal alerts and externally received information about vulnerabilities [6]. Recent years have demonstrated a trend towards the building of communities for the semi-automated exchange of CTI [7]. Automation is the key to successful CTI sharing but there are no mechanisms available to automate large-scale information sharing [8]. Current threat intelligence platforms provide limited mechanisms for automation [9]. According to the Ponemon Institute survey conducted in 2014, 39% of participants answered that slow and manual sharing processes impede full CTI exchange participation. 24% answered that slow and manual sharing processes keep them from sharing at all [10]. For example, slow and manual processes may be copying and pasting spreadsheets or meeting other peers to share information. Data processing is mainly done manually because analysts have to evaluate the problem [11], implement the solution, and share the information. Manual data preparation is labor intensive and time consuming, and renders information rapidly obsolete. The

analyst has to prepare the information for sharing with trusted stakeholders. Not only the outgoing information has to be manually prepared, but also the incoming intelligence has to be analyzed regarding content relevance, trust in source and stakeholder, impact, and other factors relevant to the stakeholders. For example, the risk priority at the end of the analysis defines the triage of the CTI. Human errors, such as miscommunication, are limited through automation [12]. The analyst can, in the near future, not be completely replaced, but support systems for automated exchange, analysis, and decision making enhance the efficiency of sharing and thus, thwarting cyber attacks.

Automated data analysis, collaboration, and sharing of CTI is imperative to cope with current and future cyber attacks [2]. The aim of automated CTI exchange is to simplify and speed up the sharing process, documentation, assessment, and remediation of security information [13]. Stakeholders are having different resources available on how much they can spend on detection and defense. Ergo, inequality in the quantity and quality of the intelligence is predictable. The course of action is therefore important to stakeholders who do not possess the financial requirements to further analyze threat information. Tagging and classification during the collection are essential for effective search and discovery as well as identifying trends through statistics, more advanced data analytics, and visualization [5]. The scarcity of experts to analyze the gargantuan supply of threats [14] and the resulting increase of data [15] emphasizes the need for automation. Promising and widely accepted protocols in the community developed by the US Government and Mitre are the Structured Threat Information Expression (STIX)[3] and the Trusted Automated eXchange of Indicator Information (TAXII)[4]. It addresses structured cyber security needs such as, analyzing cyber threats, specifying indicator patterns, managing response activities, and sharing of cyber threat information [16]. The European Telecommunications Standards Institute (ETSI) follows up on the European Union Agency for Network and Information Security (ENISA) recommendation[5] for European Union member states to implement the globally accepted CTI sharing standards STIX/TAXII [17]. Nevertheless, other languages to describe and share CTI have been published [18]. Table 1 lists some of the most popular languages for CTI description and sharing.
A note on priority, actionable intelligence is appreciated but automated defense in response to intelligence is preferred [14].

The following use case depicts automated sharing:

- Organization A is setting up a threat intelligence sharing program to gather information about relevant vulnerabilities. A Threat Intelligence Platform (TIP) is used to connect to CTI repositories, visualize their content, and correlate archived information with newly sourced one. Organization A received information about the “Ursnif bank ing malware downloaders” which install further malware from “http://mondaynightfund

[3]Structured Threat Information Expression (STIX): https://tinyurl.com/ybjgmoc7

[4]Trusted Automated eXchange of Indicator Information (TAXII): https://tinyurl.com/ybjgmoc7

[5]The Directive on security of network and information systems (NIS Directive): https://tinyurl.com/jpw7kqz

Title	Description	URL
Structured Threat Information eXpression	Structured language for CTI sharing (human and machine readable in JSON)	https://tinyurl.com/ybjgmoc7
Trusted Automated eXchange of Indicator Information	Language to share CTI (open transport mechanism with native support for HTTP and HTTPS)	https://tinyurl.com/ybjgmoc7
Open Threat Partner Exchange (OpenTPX)	Open source language that supports machine-readable threat intelligence sharing in JSON	https://tinyurl.com/yd5uopkc
Malware Attribution Enumeration and Characterization (MAEC)	A standardized langauge for sharing structured information about malware (human and machine readable in XML)	https://tinyurl.com/yb35uj9k
Incident Object Description Exchange Format (IODEF)	Framework for sharing computer security incidents in XML	https://tinyurl.com/ych8ekus
Vocabulary for Event Recoding and Incident Sharing (VERIS)	Language to describe structured security events	https://tinyurl.com/y9uvh9yx

Table 1: CTI Protocols

arts[.]com/images/Nu48djdi". The stakeholder can now search for affected downloaders in the system and block the malware site before it becomes infected.

2.2. CTI Sharing Collaboration

A CTI sharing collaboration is being built between stakeholders, as a peer-to-peer, peer-to-hub, or a hybrid exchange (Figure 2).
These stakeholders share similar interests in attack patterns or belong to the same industry sector. To be more effective, future cyber ecosystems should include security capabilities built into cyber devices that allow preventive and defensive course of actions to be coordinated within and among communities of devices [19]. To effectively exchange CTI, stakeholders need to use an exchange model which is realistically coupled to technology. Most stakeholders would like to share cyber intelligence, but successful models are missing [2] or are incomplete. To be effective, CTI should be exchanged globally, but cultural differences may impede the threat exchange. Challenges lie in the communication, in the language itself, and comprehension of specialized words. Members usually come from different backgrounds and even speak different languages which can negatively effect the quality of the knowledge [20]. A common reason why organizations do not share their CTI is that they

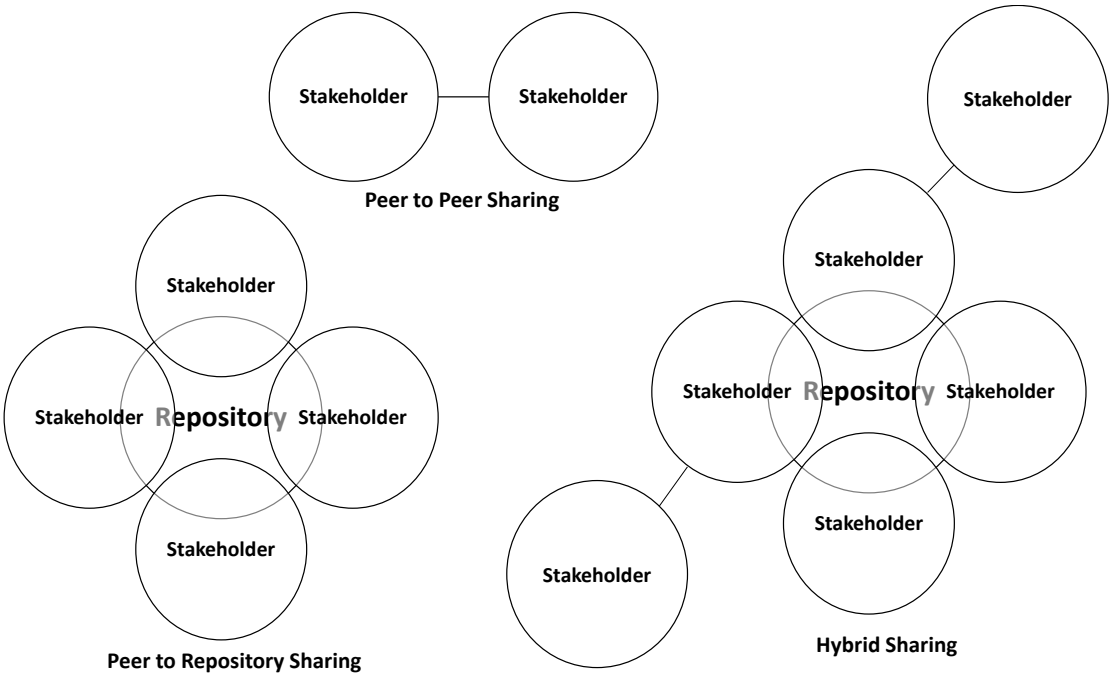

Figure 2: Sharing models: This figure visualizes the 3 common models in CTI sharing. Peer-Peer allows for direct CTI sharing. Peer-Repository (hub-spoke) enables peers to subscribe to published events. Hybrid sharing combines the aforementioned models.

believe they do possess nothing worth sharing and that competitors use the information against them [21]. Very limited support for efficient collaboration is presently available [8]. Mandatory CTI exchange may be enforced by various governments to enhance sharing and improve CTI quality. Benefits of mandatory sharing are the advise from authorities on how to effectively invest in preventive and detective measures, and authorities can warn firms regarding ongoing threats [22]. Organizations that have been targeted by state-sponsored attacks require a closer sharing and collaboration with the government [23]. According to the European Union Agency for Network and Information Security (ENISA), 80 initiatives and organizations and more than 50 national and governmental Computer Security Incident Response Teams (CSIRTs) are involved in CTI sharing at European Union (EU) and European Economic Area (EEA) level [24]. Many organizations have discovered that CTI exchange is a necessity to survive future attacks rather than a fad. Governments, including EU member states, the United States, Japan, and Korea, have made efforts to enhance and expand information sharing [25]. According to a survey from 2012, 35% of Computer Emergency Response Teams (CERTs) share their incident data, 33% automatically correlate incidents, and 40% use the shadowserver foundation as an external source [6]. In the United Kingdom, the Cyber Security Information Sharing Partnership (CiSP) initiative had 777 organizations and 2,223 individuals joined by 2014 to share knowledge about security incidents [26]. On the negative side, collaborated CTI exchange can also be a privacy risk when data is shared on an application level. It may contain private information that could be sold on the dark web [27]. If an organization does not participate in any form of threat

intelligence sharing or consumption, the increasing attacks may damage an entity beyond oblivion. This may be mitigated by producing and consuming threat intelligence. The loss or damage of assets can be devastating to an organization, but also the resulting reputation and brand damage can provoke further damages and thus, act as an incentive [28]. The research in [29] presented a U.S. patent pertaining to the collection, analysis, and distribution of CTI in 2002. This was one of the first frameworks to share information about security vulnerabilities. The research in [30] presented a game theoretic model for CTI sharing in the cloud. The model focused on trade-offs between the security and risks of sharing CTI. Furthermore, the model calculates the motivation of stakeholders to share CTI when they are easy to discover. The work in [31] introduced a category theory based approach to share threat intelligence using STIX. Furthermore, the authors extend their model by using the Functional Query Language (FQL) to make their model more practical. The research in [32] presented a threat sharing model for developing countries, i.e., South Africa. The platform focuses on the collection, analysis, and classification of CTI. Including the integration of external tools such as anti-virus software and intrusion detection systems. The 4 previously presented works contributing to CTI collaboration from various perspectives. Where [29], [30], and [31] are applicable to generic CTI collaboration; [32] focuses on specific CTI sharing collaboration pertaining to environmental needs, i.e., country specific.

2.3. CTI Indicators

CTI contains various attributes which renders it into actual intelligence. Malicious IP addresses or hashes on their own are not considered CTI but may be part of it. Attributes may include descriptions of threat actors, campaigns, motivation and Indicators of Compromise (IoC) which can be shared with trusted stakeholders. IoCs are one of the easiest actionable CTI attributes and are the focus of most tools [3]. Actionable CTI IoCs are commonly used in applications such as Intrusion Detection Systems (IDS), website blocking, blackholing, identifying compromised hosts and malware [33]. CTI libraries that store indicators are used to link historic indicators to newly discovered ones using big data technologies [21]. CTI indicators focus on enterprise IT and neglect newer fields such as the Internet of Things (IoT), Industrial Internet of Things (IIoT) and the automotive area. Nevertheless, these devices, or embedded devices, are connected to the back end and may benefit from CTI indicators that were intended for the enterprise IT.

2.4. Industry Sector Sharing

Governments and organizations have created industry specific sharing groups such as in the, inter alia, finance, retail, academia, automotive, electricity, and industrial sectors to share specific CTI. These groups are trying to mitigate sector specific vulnerabilities [34] such as card payment vulnerabilities in the financial and retail sector, and car software bugs in the automotive sector. The following use case describes a threat in the automotive sector and how to mitigate the threat through CTI sharing:

- The infotainment system is a critical part of the car. It can be accessed through a cell phone, and may contain Personally Identifiable Information (PII). A vulnerability

inside the cell phone's application was detected by Stakeholder A, a member of the AUTO-ISAC, who shared the information immediately. Stakeholder B, a further member, used the provided information to detect a vulnerability in a similar application. The vulnerability was ameliorated before it could be abused.

The research in [35] describes the sharing across the domains as "boundary objects", which span the boundaries of the practices of communities that are commonly understood by all communities. "Boundary objects" means that information can be used by different communities [36], or CTI sharing industry sectors. The advantage of sector sharing is that a problem can be solved together in real time [25]. Furthermore, CTI is more relevant to stakeholders due to similar systems and vulnerabilities. Organizations and institutions are heterogeneous and represent different interests [37]. Hence, with sharing sectors and groups a common interest in threats and vulnerabilities can be achieved.

According to [38], 56% of stakeholders receive CTI from vendors, 54% collect intelligence from public CTI feeds, and 53% gather CTI from open source feeds. The work in [14] describes the core elements of CTI sharing in two steps. CTI exchange has to be relevant and actionable, the threat sharing model has to be speedy, scalable, and automated. The research in [19] describes the core elements of CTI sharing as secure, environmentally sustainable, and rapidly customizable. Information exchange can become challenging if stakeholders use different data formats, structures, labeling options, and turning data into knowledge comprehensible to everyone. Knowledge can be externalized and reconceptualized before being shared [2]. A healthy CTI exchange implies a secure exchange, environmentally sustainable, rapidly customizable [19], correct labeling, anonymity, relevance, trust, and confidentiality. CTIs tactical intelligence exchange includes Techniques, Tactics, and Procedures (TTP) and IoCs. IoC may contain information about malicious IP addresses which are trivial to share [3] compared to, for instance, information about the techniques of an adversary. Nevertheless, strategic intelligence is rarely shared because it could reveal information about the stakeholders strategic plans [21]. The researchers in [39] presented a use case for strategic CTI sharing from Intrusion Detection System (IDS) logs. The data was collected from sources such as, honeypots, incident reports, and logs.

Groups of common interest or industry sector are built to share specific CTI. For example, the FI-ISAC requires stakeholders to attend meetings, members may be excluded if they fail to attend three successive meetings [24]. The work in [6] suggests that it may be reasonable to assume that stakeholders do not come to an agreement to use a single CTI exchange standard. Which would mean that a Threat Intelligence Platform (TIP) would need to be adoptable to different standards.

TIPs have flooded the market and made it challenging for practitioners to decide which one to implement. The TIPs in Table 2 are some platforms that currently establish their position in the CTI sharing world. The platforms differ slightly in layout, nevertheless, offer similar functionalities to visualize CTI records, correlation, tagging, feeds, and data format support.

TIP	Focus	URL
Malware Information Sharing Platform (MISP)	General CTI sharing	https://tinyurl.com/y9zgp67g
NC4 CTX/Soltra Edge	Financial CTI sharing	https://tinyurl.com/yajjrjfk
ThreatConnect	General CTI sharing	https://tinyurl.com/yaywybkm
AlienVault	General CTI sharing	https://tinyurl.com/yajehh6e
IBM X-Force Exchange	General CTI sharing	https://tinyurl.com/yc45dbdl
Anomali	General CTI sharing	https://tinyurl.com/y86volhm
Facebook ThreatExchange	General CTI sharing	https://tinyurl.com/yc6xsqxp
CrowdStrike	General CTI sharing	https://tinyurl.com/y9zkc5wy
ThreatQuotient	General CTI sharing	https://tinyurl.com/y7xd7kjv
EclecticIQ	General CTI sharing	https://tinyurl.com/ydfckucr

Table 2: Threat Intelligence Platforms

2.5. Benefits of CTI Sharing

Some organizations still hesitate to share their CTI because of missing incentives [40], but expect to receive knowledge from other peers in the community [20]. Once an organization was the victim of a cyber attack, the loss of reputation and the resulting brand damage may encourage stakeholders to invest more into cyber security and sharing CTI [28]. Automation itself can act as an incentive or a financial model could be implemented [2]. Another incentive emanates from the cost savings of CTI sharing by knowing the threat before the attack happens [41]. A successfully defended network may contribute to the up-time and continuity of the service. The researchers in [42] are discussing the effect that joy, enthusiasm, energy, and happiness can have on sharing activities. The work in [43] conducted research into the incentives for revealing security information. The research uses a prisoner's dilemma scenario which revealed that the disclosure costs lead organizations to exhibit free-riding behavior. Nevertheless, organizations would prefer full disclosure of CTI on both sides. Organizations are naturally heterogeneous and capabilities of generating and sharing intelligence differ. Hence, an equal amount or quality of knowledge is unrealistic. Involving organizations into a threat sharing collaboration can be a tedious task for several reasons. Inappropriate threat sharing models, sharing with competitors might deter stakeholders, one-way flow of information [23], revealing data breaches, and investing time and money into a threat intelligence team may seem inappropriate pertaining to the return on investment at first sight. It is surmised that members increase their contribution in expectation to be rewarded for it in form of reciprocity [20]. The work in [44] suggested a punishment model which inclines isolation from the threat sharing community. If an entity decides not to share, and only consume, CTI, then the punishment process will revoke permission rights. If the stakeholder decides to rejoin the threat sharing community, then he will only be able to contribute intelligence for a specified time until consumption may commence again. The US Congress proposed a tax credit act (Cyber Information Sharing Tax Credit Act (USA)) which is a financial incentive in form of a tax credit for organizations which share CTI with other Stakeholders. The act was introduced by Senator Kirsten Gillibrand

in July 2014 [45]. Providing a trusted environment for stakeholders is a key attribute for CTI sharing. Therefore, trust management may be an incentive to establish collaborations between stakeholders [46].

2.6. Risks of Sharing CTI

CTI sharing promises to be another tool in the cyber defense system, nevertheless, it comes along with certain risks. Sharing CTI with unauthorized stakeholders, or even inside the organization, may become a risk which could deter stakeholders from automation [2]. According to a case study from [47], some organizations were concerned that they might become a target if they were discovered as active CTI exchange members. This worry has not been proven yet by any academic research and no cases are known that would confirm an attack based on these concerns. The authors in [48] defined three implications stakeholders may face when sharing CTI. Sharing CTI with competitors might encourage free riding and not sharing information with the stakeholder or collective, trust might be violated, and negative publicity may affect market value and stock price. The researchers in [49] raised concerns that the disclosure of internal information related to an incident may harm a stakeholder's reputation. Internal information may include e-mail addresses, names, and other PII. CTI that was intercepted by an adversary could be used to attack stakeholders who have not yet patched their system [50, 51]. Every shared information should have a risk calculation according to its sensitivity and impact. The CTI sharing model in [52] has risk level values between 1 (low risk) and 20 (high risk) and eradicates links between stakeholders if the risk level is unacceptable. For instance, if stakeholders share CTI cross-border, then a higher risk level is automatically applied than to a stakeholder from the same country.

2.7. The Human Role in CTI Sharing

To render CTI sharing more effective, pertaining processes have to be automated as much as possible. Nevertheless, this ambition may not be completely fulfilled in the near future. The identification, remediation, and prevention process still requires a human user in the operation [4]. Analysts still have a lot of copying and pasting to do which limits the time available to focus on threat analytics. Furthermore, tacit knowledge about cyber threats is onerous to share with other stakeholders [42]. Tacit knowledge is inside the analyst's mind and hence challenging to capture and automate. The way one stakeholder sees a threat might not be the same for another one [53]. Stakeholders have diverse ambitions and behaviors regarding CTI sharing. The researchers in [54] define behavior in two categories, obedient or malicious. Obedient stakeholders follow the regulations and policies, malicious do not. Malicious stakeholders may use the collected CTI to attack an obedient stakeholder. Face to face meetings contribute to trust establishment between stakeholders. This may be a necessity at the beginning but may not be seen as efficient if the sharing process is not automated [26]. The work of [55] analyzed the human behavior during CTI sharing. The theory of planned behavior was used to characterize employee commitment towards CTI sharing. Furthermore, humans may withhold facts about threats because they think it is not safe for sharing for fear of being exposed [56]. The research in [57] illustrates that

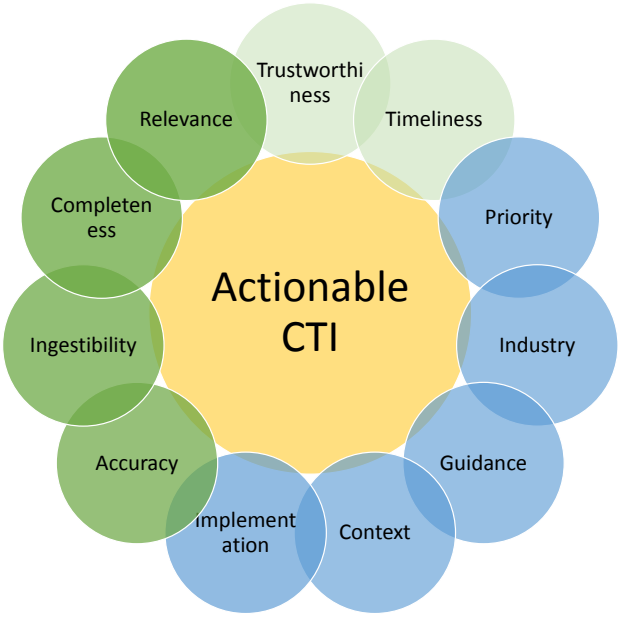

Figure 3: Actionable Cyber Threat Intelligence. Green denotes ENISAs definition; blue denotes Ponemon's definition; light green denotes ENISAs and Ponemon's overlapping definition.

information-seeking stakeholders turn to the information of weak peers if information from strong peers is unavailable. It is mentioned that heterogeneous information from weak peers may be more useful than homogeneous information from strong peers.

2.8. Cultural and Language Barriers

CTI exchange is performed globally and can cause cultural and language barriers between stakeholders. A sharing language, most likely English, has to be defined and cultural aspects have to be understood and respected. The differences may negatively affect the quality of knowledge [20]. Speaking the same tongue may encourage stakeholders to share their intelligence and can boost the knowledge sharing process [58]. Non-native speakers may face challenges to explain threats in appropriate English. Certain core attributes may be lost in translation and could decrease the CTIs quality and relevance. If the language is not understood by the stakeholder than a time consuming translation has to be initiated. The work in [59] conducted research into the behavior of CTI sharing in the US American and Swedish culture. The findings revealed that US American organizations tend to a stronger association to structure and control than coordinating processes pertaining to CTI sharing; oppositely Swedish organizations tend to prefer coordinated processes and CTI sharing.

3. Actionable Cyber Threat Intelligence

Receiving and submitting information about vulnerabilities requires several processes before CTI can be called actionable. ENISA defines actionable CTI that fulfills five criteria: relevance, timeliness, accuracy, completeness, and ingestibility [11]. Equivalent to the previous definition by the Ponemon Institute, actionability stands for timeliness, priority,

implementation, trustworthiness of the source, relevance to the industry, clear guidance to resolve the threat, and sufficient context [60] (Figure 3). These attributes define the current actionability of CTI.

From these two definitions we can derive that relevance of the information is one part of the actionability. Relevance most likely stems from the content relevance, meaning the threat is a risk to the system. Relevance may be a synonym for completeness and trust, because if the stakeholder is not trustworthy and the information is incomplete, then it may not be considered relevant. Timeliness is mentioned by both sources which stands for sharing and receiving up-to-date information in a timely fashion. Timeliness is subjective to every single stakeholder and can therefore affect the actionability outcome. Accuracy of the information can only be evaluated after the analysis but should tell the stakeholder or the machine how to proceed exactly to remedy the vulnerability. To complete the actionability, the risk level priority has to be defined. This depends on the organization's system and is subjective to the stakeholder's mindset or the machine's program. The types of CTI consumers are different and so is the relevant information to each one. The research in [5] identified four stakeholders who work with CTI. Namely high level executives, threat managers, threat analysts, and incident response teams. CTIs data quality may differ by sharing stakeholder or source. The Quality may be evaluated by the correctness, relevance, timeliness, usefulness, and uniqueness [50]. Furthermore, a member of the CTI sharing community who has always shared useful and timely information may be labeled as a quality stakeholder [51].

3.1. Timeliness of Sharing CTI

Some cyber attacks occur in seconds at various sites using the same or similar attack patterns. A swift information sharing process is an important attribute of CTI exchange because of the narrow response time frame [11]. The sharing and reacting processes have to be adequate according to the limited time frame. The threat environment changes quickly and thus, CTI must be acted upon quickly. The importance of sharing in a speedy manner can be observed when the value of CTI goes to zero in days or even hours [3]. As shown in previous research, 60% of malicious domains have a life span of one hour or less [61]. Timeliness does not only focus on age, but also on frequency of updates to threat activities, changes, or evolution in capability or infrastructure [62]. The following use case illustrates the importance of timeliness:

- Scenario A: Organization A immediately shared CTI within the trusted repository after detection. The shared information was received in a timely manner, but due to the incomplete Course of Action (CoA), stakeholders were unable to make use of it.

- Scenario B: Organization B detected an indicator (Locky Downloaders) about a malicious link inside an e-mail that, once clicked on, downloads a Trojan horse onto the victim's machine and stays undetected by conventional anti-virus programs. The information was shared in a matter of seconds within the trusted circle of peers. The stakeholders were able to promptly mitigate the risk by blocking the e-mail and link.

3.2. Trust Establishment of CTI Sharing

Establishing a CTI sharing collaboration requires a comprehensive trust relationship between stakeholders. Trust is normally established over time and in face-to-face meetings. The challenge here lies in trust establishment amongst decentralized stakeholders. Trust is a key attribute in the CTI exchange ecosystem and challenging to rebuild when broken [41]. It is considered the most difficult attribute in the threat intelligence sharing ecosystem [52]. CTI can contain information that should only be revealed to trusted stakeholders or not at all, such as PII which is irrelevant to create situation awareness. Information about a successful attack getting into the wrong hands can have a disastrous impact on the reputation of the stakeholder. It can be used against the organization if the countermeasure has not been implemented yet. The trustworthiness of a stakeholder is evaluated through trust and reputation, where trust is established through direct contact and reputation from opinions of other peers [63]. According to [64], three trust relationships were identified: Organizations trust platform providers that (1) confidential data is not exposed to unauthorized stakeholders; (2) correct handling of information, such as TLP labeling; (3) Shared information is credible and reliable. The research in [9] showed that there are two possible perspectives on trust, the organization perspective and the provider perspective. Stakeholders may show a benign behavior at the beginning and later on start to abuse the trust. Thus, it is onerous to identify peers with benevolent or malicious intents [65]. The work of [66] identified a trust scheme which is applicable to virtual identities: reputation, past outcomes, degree of activity, degree of connectivity, regularity, stability, and accountability. The work in [67] elaborated further on the reputation scheme that identifies slander attacks where malicious nodes intentionally provide negative evaluations to normal nodes and collusion attacks where acquainted nodes give each other positive evaluations. The research in [20] discusses the three dimensions for trust: ability, benevolence, and integrity based on the work in [68]. Trust relationships may be managed by trusted third parties such as threat intelligence vendors or may be outsourced by utilizing a trust manager to handle reputation [69]. Trust concerns can arise when the government is involved in CTI exchange or the development of tools and protocols. For example, STIX and the Trusted Automated eXchange of Indicator Information (TAXII) have been developed by the Mitre group with the support of the US Government. This collaboration could deter stakeholders from countries other than the US to trust these protocols [34]. Since the tendency of not trusting the government in the United States is prevalent amongst US citizens, it may even keep US companies from adopting these tools. Low level risk threat intelligence can be shared in centralized form but decentralized exchange requires a greater degree of trust [23], or a limit to the number of participating stakeholders [24]. According to [11], the three trust levels are defined as: high level of confidence from trusted and fully verified channels, medium level of confidence for reliable channels, and low confidence for unverified data sources. Another aspect of trust relationships is that they are mostly built between individuals and not companies. Thus, if the responsible employee for CTI sharing decides to leave the organization, then all of her contacts may leave too. The work in [25] defines the trust base as stakeholder contribution, collective actions, and shared experiences. The research in [70] outlines the trust evaluation process in two ways: as situation specific where trust is established regarding a specific

type of information; person specific regarding the judgment of two stakeholders on the same matter. Moreover, stakeholders have to indicate their individual degree of confidence in the credibility and accuracy of the CTI [71].

The following scenario describes a "sleeper" attack scenario which builds up trust over time only to exploit it at the right moment.

- Scenario A: 423 Stakeholders have established a trusted relationship with focus on the retail industry and its vulnerabilities. CTI sharing has been conducted for several years without any trust conflict and stakeholders have revealed system specific details pertaining to vulnerabilities. One of the stakeholders had a malicious intent to exploit the other stakeholders. They waited for several years to enhance the trust level and to access classified CTI. Open vulnerabilities were exploited by the "trusted" stakeholder as a result of the long term gained trust.

Lessons learned: Sharing systems need to have a continuous vetting process in place to detect malicious peers at an early stage. Furthermore, stakeholders should anonymize their content as much as possible and hide system specific details.

3.3. Stakeholder Reputation

Stakeholders have to build up their reputation to become trusted members of a threat sharing community. Reputation is built over time by sharing high quality and actionable threat information, and conforming to threat sharing policies. There are many ways to build up a reputation to earn credibility amongst other stakeholders. To increase the credibility, stakeholders have to continuously share CTI, correlate various sources, and respond to questions by the community pertaining to the shared intelligence [41]. On the contrary, once a bad reputation has been entrenched it is challenging to reverse the effect. To the best of our knowledge, no research has been conducted regarding negative reputation in CTI sharing. Thus, research from neighboring fields is considered. One such field is the online retail sector where sellers and buyers rate each other according to the quality of product, deliver speed, communication, payment, and accuracy of description. The quality of the bought tangible product can be matched to the quality of the shared CTI; the delivery speed of the mailed product may be compared to the sharing speed of CTI; seller/buyer communication can be correlated to questions by the consuming peer regarding a set of CTI; and accuracy of product description can be paralleled to the description of CTI indicators. If a seller or buyer has received negative feedback, other peers may be encouraged to negatively comment as well, having received similar poor service [72]. This process is called stoning and helps to separate good from bad peers [73].

3.4. Relevance of CTI

Due to the uncountable number of threat indicators an analyst would be completely overwhelmed by all the data. Therefore, a scalable relevance filter has to be used by stakeholders. Sharing too much information is as bad as sharing too little. Hence, suitable

filtering methods have to be implemented [71]. The work in [11] defines relevance as that CTI must be applicable to the stakeholder's area of responsibility, including networks, software, and hardware. Furthermore, data relevance is an important factor of data quality [5]. Current relevance filtering is based on manually selecting high level CTI which is seen as important and browse/search functions are enabled in TIPs and online platforms. Stakeholders have to understand and define which CTI is relevant to their system by knowing their inventory. Threat types should be analyzed whether they are targeting stakeholder assets. Business processes ought to be mapped according to geographical, political, and industry sector [62]. Irrelevant information is not shared with other stakeholders, but it is stored in the local knowledge base and correlated with new information [35]. The research in [74] presented a scalable content filtering and disseminating system which could be implemented into a CTI sharing environment. Another area of information filtering is SPAM filtering, where [75] contributed a content based SPAM filter. The relation between SPAM and CTI is that stakeholders do not want to receive SPAM e-mails, but only genuine messages. The same statement is valid for CTI, where stakeholders only want to receive relevant information (genuine e-mails) and not irrelevant information (SPAM). Stakeholders should have full control over what type of CTI appears on their feed. In comparison, social networks are flooded with information but only a fraction of it is actually relevant to the user [76]. On these platforms users have direct control over which messages are posted on their walls by customizing the filtering criteria [77]. The work of [78] researched the problem of information filtering in peer-to-peer networks. The focus here lies on the information filtering functionality with low message traffic and latency. The research in [79] presented the CyberTwitter framework which collects Open Source Intelligence (OSINT) from Twitter feeds. The evaluation of the tool comprised the quality of the threat intelligence and whether relevant information was missed.

- Scenario A: Stakeholder A receives 15,000 threat alerts per week from its monitoring system. 400 alerts are considered relevant and 60 are investigated due to an employee shortage. Moreover, the stakeholder receives further 10,000 threat alerts that are considered high risk but may not be relevant to the system.
- Scenario B: Stakeholder B receives about the same amount of alerts per week and has similar capabilities to investigate as stakeholder A. Nevertheless, the stakeholder uses a tagging system to render the CTI content relevant to its system. This approach saves time and makes CTI sharing more effective.

Lessons learned: CTI has to be rendered relevant to individual stakeholders because of the heterogeneity of systems. A tagging system may provide the necessary basis to render CTI content more relevant. Content relevance is one of the attributes of relevance.

3.5. Privacy & Anonymity

Organizations have to prioritize privacy of clients by sharing CTI only with trusted stakeholders and/or anonymize the content. Several matrices were developed to anonymize

the content of information such as k-Anonymity [80], l-Diversity [81], t-Closeness [82], ϵ-Differential privacy [83], and Pseudonymization [84, 85, 86]. Stakeholders are still reluctant to share information about breaches because of fear that it could damage their reputation which is an important asset to protect [46]. Another aspect of anonymity is the encryption of CTI when shared between stakeholders. A Man-in-the-Middle attack could intercept the shared information. A protocol for encrypting CTI called PRACIS was presented in [87]. PRACIS enables privacy preserving data forwarding and aggregation for semi-trusted message oriented middleware. The work in [88] presented an architecture to compute privacy risk scores over CTI. The research discusses the privacy risks of extracting personal information from threat intelligence reports. Both presented works may be merged to enhance privacy in a CTI program.

Anonymous sharing is imperative in certain circumstances when a stakeholder does not want to reveal yet that their system was breached, but wants to share the information with other stakeholders. Further, when trust has not been established yet then anonymous threat sharing is desirable. Anonymity of CTI has to be established within the content, meta data, and data transfer. The content should not contain any PII about the organization, employees, and its clients. The current method of content anonymization is manual screening for PII that should not leave the organization's premises, or even be read by unauthorized internal employees. Automating the anonymization process can be achieved by using regular expressions to find PII [89]. Every stakeholder has a different perception of anonymity. What might be sensitive information for one stakeholder might be trivial for another. Ergo, adjustment of masking criteria and scalability are important factors for appropriate anonymization. Sharing raw data could reveal sensitive information about individuals or about the operation context [51]. Moreover, anonymizing the content is not enough to provide sufficient privacy. The connection has to be anonymized as well and one possible approach is to route the connection through the TOR network [90]. The server should not have been connected previously to the clearnet, which could have left traces on the server that could identify the stakeholder. Additionally, the browsing behavior has to be adjusted to avoid accidental disclosure of the identity. The research in [91] concentrated on preserving IP address anonymization using a canonical form and a novel cryptography based scheme, which could be applied to anonymous CTI sharing. Encrypting CTI could prevent critical information to be revealed and used against stakeholders before the vulnerability was remedied. This is called implicit privacy where the attacker cannot directly use the information, it would have to be analyzed first [63], or decrypted. Information consists out of different attributes and with contrasting levels of sensitivity. Further, knowledge of the existence of CTI can have a different level of sensitivity than its content [71]. The following two scenarios provide an insight into anonymous CTI sharing:

- Scenario A: Stakeholder A does not use any form of anonymity in its CTI sharing process. Hence, PII is constantly revealed to other CTI sharing stakeholders. The stakeholder connects to trusted sources but also to repositories which do not have a vetting process in place. Besides, the CTI may contain details about unremedied vulnerabilities that linger inside the system. A malicious stakeholder was able to collect

various CTI from stakeholder A over a couple of months. The correlated information revealed the identity of stakeholder A and where they are vulnerable. The attacker was therefore in the position to successfully exploit the vulnerabilities.

- Scenario B: Stakeholder B anonymizes its content by masking PII such as e-mails, company name, and IP addresses. Moreover, shared CTI is exchanged in encrypted form to enhance privacy. A Man-in-the-Middle attack intercepted the shared information which contained highly classified details about the organization's system and how to exploit it if the vulnerability is not remedied. Due to the encrypted data, it took the attacker several months to crack the encryption which rendered the information useless. Until then, the majority of stakeholders already remedied their systems against this specific attack.

Lessons learned: Stakeholders have to ensure that a certain degree of anonymity is provided when CTI is shared. This depends on the criticality of the information and with whom it is shared.

3.6. Data Interoperability

A note on interoperability, numerous organizations want to share their CTI but a globally common format for CTI exchange is absent [12]. Data formats have to be compatible with stakeholders contrasting systems. Therefore, a common format has to be agreed on by all stakeholders. According to an ENISA study from 2014, there are 53 different information sharing standards that have been adopted by the community [92]. Unnecessary data transformation has to be avoided which could impede the timely exchange of CTI. Standards have to be developed [2] and accepted by the community. According to [14], interoperability is becoming important but not necessary the desired default state because it gives developers the diversity in data formats. The Mitre group developed the STIX format to render CTI exchange interoperable [34, 16]. It has become the most widely accepted standard for threat intelligence sharing. Besides the data format interoperability, the information sharing infrastructure has to be flexible enough to cope with a variety of implementations [93].

4. Cyber Threat Intelligence Sharing Regulations

Sharing information about cyber threats requires a combination of technical and policy methods [94]. If an organization decides to share their CTI, a clausal for information has to be included or updated in existing policies [4]. All information exchange with other stakeholders has to go through the Information Exchange Policies (IEP) which is an internal document [8]. The research in [95] identified the following elements that have to be included in the IEP: purpose, scope, participants, procedure for new stakeholders, information about handling of received data, procedure for IEP modification, requirement for data sharing, uses of exchanged data, mechanisms, and intellectual property rights. The research in [96] analyzed the Data Sharing Agreement's (DSA) defining terms: data quality, custodial

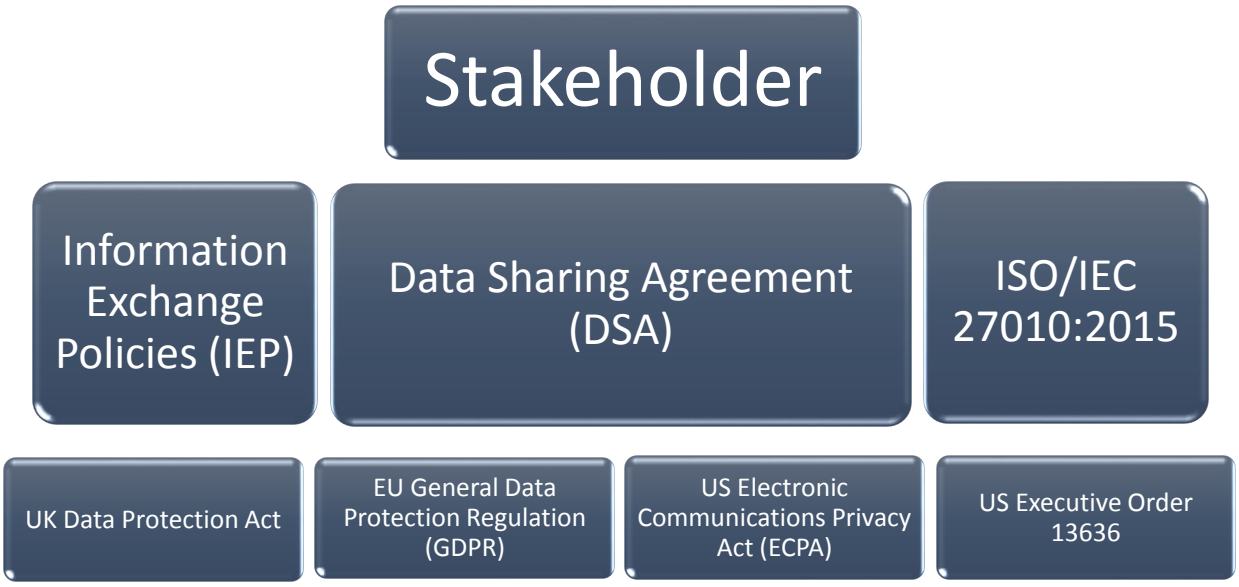

Figure 4: Regulation Hierarchy for Cyber Threat Intelligence Sharing

responsibility, trust domain, and the security infrastructure. The British Standard ISO/IEC 27010:2015 Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications provides guidance for stakeholders to share their information [71]. Ethics in data sharing has to be part of the information sharing policy. Stakeholders have to define for which purpose the CTI is used, who can access it, retention periods and destruction, and condition of publication [97].

4.1. Laws and Regulations of CTI Sharing

CTI is exchanged globally which means that laws and regulations of various countries have to be considered. CTI can contain information that is legal to share in one country but illegal in another [13]. For instance, according to the UK Data Protection Act, IP addresses are not considered personal information. Quite the contrary, a German court decided in 2016 that IP addresses are personal information in some cases[6]. Organizations have to ensure that they comply with country privacy laws and when CTI is shared with foreign stakeholders. Depending on the country, organizations may face penalties for not sharing security breaches with the authorities and affected individuals [22]. For instance, in Slovenia based on the Electronic Communication Act, the Communications Networks and Services Agency (AKOS) is obliged to notify vulnerabilities to the national and governmental CSIRT (SI-CERT). In Belgium, public electronic communications services have to report vulnerabilities to the national regulator of electronic communications [24]. Legal action may also be taken against Stakeholders who do not act on CTI and thus are breached. Stakeholders who do not participate in threat sharing programs could also be punished

[6]https://tinyurl.com/yanfkqct

[47]. Nevertheless, legal constraints may impede stakeholders from sharing their intelligence [11]. For example, internal data protection policies and country specific data protection may obstruct the sharing process. In the US, the Electronic Communications Privacy Act (ECPA) and the Foreign Intelligence Surveillance Act (FISA) have contributed to a confusion regarding whether CTI can be shared. The acts prohibit communications provider from voluntary disclosure of communications content [23]. Nevertheless, the executive order (EO13636) in the US was published in 2013 to increase information sharing [98, 99]. Figure 4 visualizes the regulations for CTI sharing based on Europe and the United States. The work of [100] researched the legal aspect of automated CTI sharing between government and non-governmental institutions, and the evolution of threat intelligence sharing which lead to the current Cybersecurity Information Sharing Act (CISA). The work in [101] discussed the privacy risks of CTI sharing in the US between the government and organizations. The research comprises a survey which was held among 76 security practitioners. The results visualize which threats security practitioners are willing to share. I.e., 24 participants were willing to share IP addresses and 3 were unwilling to share keylogging data.

CTI sharing has to be conducted with as many stakeholders as possible who share actionable threat intelligence to be more effective. Cyber attacks do not know any borders, therefore, CTI sharing should ideally not be impeded by various country regulations. A harmonized CTI sharing process may have to be adopted by various countries to make full use of the intelligence. Stakeholders are still analyzing the processes involved for effective threat intelligence sharing, and are yet in doubt what can or should be shared, and with whom. The GDPR (General Data Protection Regulation) will render it mandatory to report incidents within 72 hours in the Europe Union. For example, the GDPR states that security incidents have to be reported within 72 hours. The time starts from when the incident was considered a positive breach by the analyst. The research in [102] investigated whether static and dynamic IP addresses are personal details according to the GDPR. The findings revealed the if IP addresses are shared as threat intelligence then it can be justified in the public interest under Article 6 (1)(e) of the GDPR.

5. Summary

The aim of this literature survey was to identify the current State-of-the-Art and set future research directions for CTI sharing and its attributes. The literature search was conducted through journal databases, university catalogs, and scholarly search engines. The research topics addressed in this survey stem from real world problems that stakeholders currently face. The literature survey is intended to give the reader a larger spectrum of diverse problems pertaining to CTI sharing. Various authors thought ahead and addressed research stages in CTI sharing that have not been reached yet by the majority of practitioners. Basic hurdles still have to be overcome, such as elementary implementations of a CTI program and convincing the responsible to invest into it. Furthermore, the harmonization of monitoring and detection tools with threat intelligence platforms is a challenge in itself. Once consumption and exchange starts, stakeholders are generally overwhelmed with the sheer amount of information and ponder how to render it relevant. Various vendors

Type	Amount
Conferences, Journals, Symposiums, or Workshops	75
Technical Reports	23
Government Bills	1
Patent	1
Guidelines	2

Table 3: Literature Type

offer threat intelligence platforms which may be the first step into the CTI world by using crowdsourced intelligence from CTI repositories. The current literature trend focuses on, inter alia, how to identify and establish a successful and long lasting collaboration between decentralized stakeholders, and to automate some of the sharing processes. The literature addresses that threat sharing has gained the interest of many organizations to work more proactive instead of only reactive. The aim of CTI sharing is creating situation awareness in a timely fashion among stakeholders by being informed about potential risks to the stakeholder's infrastructure or IoT products. Automation is a preferred method by stakeholders, i.e., indicators are automatically captured, prepared, shared (with a trusted stakeholder), and automatically implemented. Some tools support the semi-automated sharing of indicators, such as malicious IP addresses and hashes. Significant work has been established with Mitre's STIX and TAXII to push the community towards one protocol for threat intelligence description and sharing. Table 1 listed other languages to describe and share CTI.

Actionability is the term used by separate sources to describe quality attributes of threat intelligence. The main attributes are relevance, timeliness, trustworthiness, completeness, and accuracy of CTI. Nevertheless, actionable CTI has different attributes depending on the literature sources.

We analyzed 102 articles, reports, and government bills with focus on CTI sharing or related areas. The tables depict a quantitative overview of the literature grouped into types in Table 3, focus in Table 4, and Figure 5 visualizes the amount of articles published per year. The types of literature are mostly academic followed by technical reports from the industry, 1 government bill, 1 patent, and 2 guidelines complete the list.

Table 4 illustrates where the focus on the analyzed topics lies. The most attention was on collaborations with 19 articles, where the authors analyzed collaborations in form of establishing a threat sharing program with decentralized stakeholders. The focus was on what information can be shared, with whom, and how to automate some of the collaboration processes. Trust has been analyzed by 17 articles and various approaches were presented to define and identify trust relationships between stakeholders. Trust in peer to peer sharing has been thoroughly researched in the past, but new challenges have arisen with the sharing of CTI. For instance, trust relationships between competitors and sharing information about vulnerabilities and security breaches. Privacy & Anonymity was also a highly sought after research topic and 17 articles of the analyzed literature dedicated their priority to it. The main topics focused on CTI anonymisation, encrypting the data, and presenting privacy risk scores. These topics have also been previously researched for related areas in

cyber security. Nevertheless, the CTI environment has changed the game for these research areas. For instance, anonymity may not be a desired function if trust has to be established between stakeholders, but in certain circumstances, anonymity may be enabled to report vulnerabilities that have not been remedied yet. Incentives also earned the interest of many authors with 12 articles. They are the basis of bringing stakeholders together who may not have met before and should share critical information about security breaches. Nevertheless, some stakeholders may not yet see the need to participate in a threat sharing program.

Focus	**Amount**
Current Threat Sharing Methods	11
Automation	7
Actionable CTI	6
Collaboration	19
Sharing	15
Timeliness	4
Trust	17
Reputation	10
Relevance	4
Privacy & Anonymity	17
Interoperability	7
Policies & Guidelines	7
Legal	9
Human Behavior	8
Cultural & Language Barriers	3
Incentives	12
Risks	8

Table 4: Literature Focus

The graph in Figure 5 portrays the amount and year of published work pertaining to CTI sharing. We analyzed what we thought relevant literature until April 2018. Works published after that date are not included. We are aware that there may be further excellent published work available that we did not include in this literature survey. Summarizing the literature timeline, between 2001 and 2009, the interest in sharing threat information was at an embryonic stage and academics and practitioners started to become interested in this emerging topic more towards 2010. 2013 has seen an increase of published literature and 2014 seemed to be the year with the most publications related to CTI sharing or related areas. 2015 to 2018 have seen a slight decline in published work.

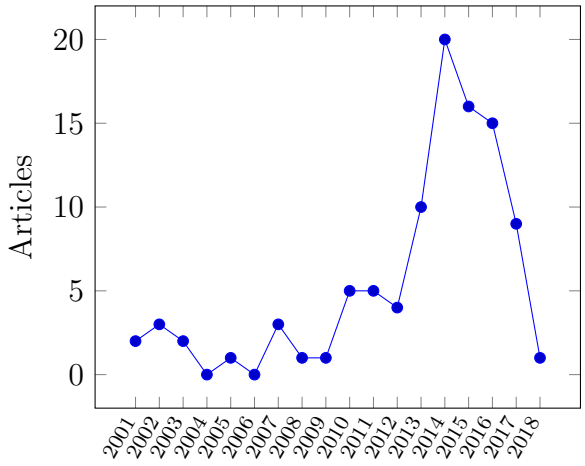

Figure 5: Literature Timeline

6. Conclusion

New methods have to be developed to thwart the steady increase of cyber attacks. CTI sharing is establishing itself to become a powerful weapon to defend against adversaries. This literature survey outlined newly emerged challenges due to an increased interest and necessity of CTI sharing. We analyzed a comprehensive amount of literature related to CTI sharing and neighboring areas where similar requirements exist. This work focused on actionable attributes and elaborated further with use cases. Regulations were discussed which support a steady threat intelligence sharing process. Furthermore, we evaluated and grouped the contributions to analyze which topics were most relevant to the authors.

References

[1] J. Sigholm, M. Bang, Towards Offensive Cyber Counterintelligence: Adopting a Target-Centric View on Advanced Persistent Threats, in: Intelligence and Security Informatics Conference (EISIC), 2013 European, IEEE, 2013, pp. 166–171.

[2] D. F. Vazquez, O. P. Acosta, C. Spirito, S. Brown, E. Reid, Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships, in: 4th International Conference on Cyber Conflict, CyCon 2012, Tallinn, Estonia, June 5-8, 2012, 2012, pp. 1–17.

[3] G. Farnham, K. Leune, Tools and standards for cyber threat intelligence projects, 2013.

[4] T. Sander, J. Hailpern, Ux aspects of threat information sharing platforms: An examination & lessons learned using personas, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, ACM, 2015, pp. 51–59.

[5] S. Brown, J. Gommers, O. Serrano, From Cyber Security Information Sharing to Threat Management, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, ACM, 2015, pp. 43–49.

[6] P. Kijewski, P. Pawliński, Proactive detection and automated exchange of network security incidents, Abgerufen am 20.

[7] C. Sillaber, C. Sauerwein, A. Mussmann, R. Breu, Data quality challenges and future research directions in threat intelligence sharing practice, in: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, ACM, 2016, pp. 65–70.

[8] L. Dandurand, O. S. Serrano, Towards improved cyber security information sharing, in: Cyber Conflict (CyCon), 2013 5th International Conference on, IEEE, 2013, pp. 1–16.
[9] C. Sauerwein, C. Sillaber, A. Mussmann, R. Breu, Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives, in: Towards Thought Leadership in Digital Transformation: 13. Internationale Tagung Wirtschaftsinformatik, WI 2017, St.Gallen, Switzerland, February 12-15, 2017., 2017.
[10] P. I. LLC, Exchanging Cyber Threat Intelligence: There Has to Be a Better Way Sponsored by IID Independently conducted by Ponemon Institute LLC.
[11] P. Pawlinski, P. Jaroszewski, P. Kijewski, L. Siewierski, P. Jacewicz, P. Zielony, R. Zuber, Actionable information for security incident response, European Union Agency for Network and Information Security, Heraklion, Greece.
[12] A. Rutkowski, Y. Kadobayashi, I. Furey, D. Rajnovic, R. Martin, T. Takahashi, C. Schultz, G. Reid, G. Schudel, M. Hird, et al., Cybex: The cybersecurity information exchange framework (x. 1500), ACM SIGCOMM Computer Communication Review 40 (5) (2010) 59–64.
[13] P. Kampanakis, Security automation and threat information-sharing options, Security & Privacy, IEEE 12 (5) (2014) 42–51.
[14] K. M. Moriarty, Transforming Expectations for Threat-Intelligence Sharing (2013).
[15] A. Cormack, Incident response and data protection (2011).
[16] S. Appala, N. Cam-Winget, D. McGrew, J. Verma, An actionable threat intelligence system using a publish-subscribe communications model, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, ACM, 2015, pp. 61–70.
[17] T. Rutkowski, S. Compans, ETSI TR 103 456 v1.1.1 "CYBER; Implementation of the Network and Information Security (NIS) Directive", Tech. rep. (2017).
[18] T. Rutkowski, S. Compans, ETSI TR 103 331 v1.2.1 (Draft)"CYBER; Structured threat information sharing", Tech. rep. (2018).
[19] B. McConnell, Enabling distributed security in cyberspace, Security Automation (2011) 8.
[20] M. Abouzahra, J. Tan, The Effect of Community Type on Knowledge Sharing Incentives in Online Communities: A Meta-analysis, in: System Sciences (HICSS), 2014 47th Hawaii International Conference on, IEEE, 2014, pp. 1765–1773.
[21] D. Chismon, M. Ruks, Threat intelligence: Collecting, analysing, evaluating, MWR Infosecurity, UK Cert, United Kingdom, 2015.
[22] S. Laube, R. Böhme, Mandatory security information sharing with authorities: Implications on investments in internal controls, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, ACM, 2015, pp. 31–42.
[23] D. E. Zheng, J. A. Lewis, Cyber Threat Information Sharing: Recommendations for Congress and the Administration (2015).
[24] B. Deloitte, J. De Muynck, S. Portesi, Cyber Security Information Sharing : An Overview of Regulatory and Non-Regulatory Approaches (2015).
[25] C. Goodwin, J. P. Nicholas, J. Bryant, K. Ciglic, A. Kleiner, C. Kutterer, K. Sullivan, A Framework for Cybersecurity Information Sharing and Risk Reduction, Tech. rep., Technical report, Microsoft Corporation (2015).
[26] S. Murdoch, N. Leaver, Anonymity vs. trust in cyber-security collaboration, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, ACM, 2015, pp. 27–29.
[27] V. Sharma, G. Bartlett, J. Mirkovic, Critter: Content-rich traffic trace repository, in: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, ACM, 2014, pp. 13–20.
[28] J. M. Bauer, M. J. Van Eeten, Cybersecurity: Stakeholder incentives, externalities, and policy options, Telecommunications Policy 33 (10) (2009) 706–719.
[29] C. Edwards, S. Migues, R. Nebel, D. Owen, System and method of data collection, processing, analysis, and annotation for monitoring cyber-threats and the notification thereof to subscribers, uS Patent App. 09/950,820 (Sep. 13 2001).
[30] C. Kamhoua, A. Martin, D. K. Tosh, K. A. Kwiat, C. Heitzenrater, S. Sengupta, Cyber-threats

information sharing in cloud computing: A game theoretic approach, in: Cyber Security and Cloud Computing (CSCloud), 2015 IEEE 2nd International Conference on, IEEE, 2015, pp. 382–389.
[31] J. Andrian, C. Kamhoua, K. Kiat, L. Njilla, Cyber threat information sharing: A category-theoretic approach, in: Mobile and Secure Services (MobiSecServ), 2017 Third International Conference on, IEEE, 2017, pp. 1–5.
[32] M. Mutemwa, J. Mtsweni, N. Mkhonto, Developing a cyber threat intelligence sharing platform for south african organisations, in: Information Communication Technology and Society (ICTAS), Conference on, IEEE, 2017, pp. 1–6.
[33] C. Ciobanu, M. Dandurand, Luc Davidson, B. Grobauer, P. Kacha, A. Kaplan, A. Kompanek, M. Van Horenbeeck, Actionable Information for Security Incident Response, Tech. rep. (2014).
[34] E. W. Burger, M. D. Goodman, P. Kampanakis, K. A. Zhu, Taxonomy model for cyber threat intelligence information exchange technologies, in: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, ACM, 2014, pp. 51–60.
[35] J. M. Ahrend, M. Jirotka, K. Jones, On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit threat and defence knowledge, in: Cyber Situational Awareness, Data Analytics And Assessment (CyberSA), 2016 International Conference On, IEEE, 2016, pp. 1–10.
[36] S. Star, J. Griesemer, Translations and boundary objects: Amateurs and professioals in berkeleys museum of vertebrate zoology 1907-39, Institutional Ecology 19 (3).
[37] R. Leszczyna, M. R. Wróbel, Security information sharing for smart grids: Developing the right data model, in: 9th International Conference for Internet Technology and Secured Transactions, ICITST 2014, London, United Kingdom, December 8-10, 2014, 2014, pp. 163–169.
[38] D. Shackleford, Who's using cyberthreat intelligence and how?, SANS Institute. Retrieved February 23 (2015) 2016.
[39] S. E. Dog, A. Tweed, L. Rouse, B. Chu, D. Qi, Y. Hu, J. Yang, E. Al-Shaer, Strategic cyber threat intelligence sharing: A case study of ids logs, in: Computer Communication and Networks (ICCCN), 2016 25th International Conference on, IEEE, 2016, pp. 1–6.
[40] C. Z. Liu, H. Zafar, Y. A. Au, Rethinking FS-ISAC: An IT Security Information Sharing Network Model for the Financial Services Sector, Communications of the Association for Information Systems 34 (1) (2014) 2.
[41] D. Feledi, S. Fenz, L. Lechner, Toward web-based information security knowledge sharing, Information Security Technical Report 17 (4) (2013) 199–209.
[42] A. Tamjidyamcholo, M. S. B. Baba, N. L. M. Shuib, V. A. Rohani, Evaluation model for knowledge sharing in information security professional virtual community, Computers & Security 43 (2014) 19–34.
[43] P. Naghizadeh, M. Liu, Inter-temporal incentives in security information sharing agreements, in: Position paper for the AAAI Workshop on Artificial Intelligence for Cyber-Security, 2016.
[44] Q. Xiong, X. Chen, Incentive mechanism design based on repeated game theory in security information sharing, in: 2nd International Conference on Science and Social Research (ICSSR 2013), Atlantis Press, 2013.
[45] C. I. S. T. C. Act, S 2717, in: 113th Congress (2013-2014)), 2014.
[46] R. Garrido-Pelaz, L. González-Manzano, S. Pastrana, Shall we Collaborate?: A Model to Analyse the Benefits of Information Sharing, in: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, ACM, 2016, pp. 15–24.
[47] J. C. Haass, G.-J. Ahn, F. Grimmelmann, Actra: A case study for threat information sharing, in: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, ACM, 2015, pp. 23–26.
[48] D. K. Tosh, M. Molloy, S. Sengupta, C. A. Kamhoua, K. A. Kwiat, Cyber-investment and cyber-information exchange decision modeling, in: High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on, IEEE, 2015, pp. 1219–1224.
[49] M. Haustein, H. Sighart, D. Titze, P. Schoo, Collaboratively exchanging warning messages between

peers while under attack, in: Availability, Reliability and Security (ARES), 2013 Eighth International Conference on, IEEE, 2013, pp. 726–731.
[50] O. Al-Ibrahim, A. Mohaisen, C. Kamhoua, K. Kwiat, L. Njilla, Beyond free riding: Quality of indicators for assessing participation in information sharing for threat intelligence, arXiv preprint arXiv:1702.00552.
[51] A. Mohaisen, O. Al-Ibrahim, C. Kamhoua, K. Kwiat, L. Njilla, Rethinking Information Sharing for Actionable Threat Intelligence, CoRR abs/1702.00548.
[52] T. Kokkonen, J. Hautamäki, J. Siltanen, T. Hämäläinen, Model for sharing the information of cyber security situation awareness between organizations, in: Telecommunications (ICT), 2016 23rd International Conference on, IEEE, 2016, pp. 1–5.
[53] D. Mann, J. Brooks, J. DeRosa, The relationship between human and machine-oriented standards and the impact to enterprise systems engineering, The MITRE Corporation, Bedford, MA.
[54] E. Anceaume, M. Gradinariu, A. Ravoaja, Incentives for P2P Fair Resource Sharing, in: Fifth IEEE International Conference on Peer-to-Peer Computing (P2P'05), IEEE, 2005, pp. 253–260.
[55] N. S. Safa, R. Von Solms, An information security knowledge sharing model in organizations, Computers in Human Behavior 57 (2016) 442–451.
[56] L. C. Abrams, R. Cross, E. Lesser, D. Z. Levin, Nurturing interpersonal trust in knowledge-sharing networks, The Academy of Management Executive 17 (4) (2003) 64–77.
[57] J. H. Park, B. Gu, A. C. M. Leung, P. Konana, An investigation of information sharing and seeking behaviors in online investment communities, Computers in Human Behavior 31 (2014) 1–12.
[58] A. Tamjidyamcholo, M. S. B. Baba, H. Tamjid, R. Gholipour, Information security–professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language, Computers & Education 68 (2013) 223–232.
[59] W. R. Flores, E. Antonsen, M. Ekstedt, Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture, Computers & Security 43 (2014) 90–110.
[60] P. Institute, Exchanging cyber threat intelligence: There has to be a better way.
[61] H. I. T. Alliance, Health industry cyber threat information sharing and analysis, Tech. rep. (October 2015).
[62] ThreatConnect, Threat intelligence platforms - everything youve ever wanted to know but didnt know to ask, Tech. rep. (2015).
[63] G. Meng, Y. Liu, J. Zhang, A. Pokluda, R. Boutaba, Collaborative security: A survey and taxonomy, ACM Computing Surveys (CSUR) 48 (1) (2015) 1.
[64] ENISA, Exploring the opportunities and limitations of current threat intelligence platforms, Tech. rep. (2017).
[65] Y. Wang, J. Vassileva, Trust and Reputation Model in Peer-to-Peer Networks, in: Peer-to-Peer Computing, 2003.(P2P 2003). Proceedings. Third International Conference on, IEEE, 2003, pp. 150–157.
[66] P. Dondio, L. Longo, Computing trust as a form of presumptive reasoning, in: Proceedings of the 2014 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)-Volume 02, IEEE Computer Society, 2014, pp. 274–281.
[67] H. Xu, Y. Liu, S. Qi, Y. Shi, A novel trust model based on probability and statistics for peer to peer networks, in: Quality, Reliability, Risk, Maintenance, and Safety Engineering (QR2MSE), 2013 International Conference on, IEEE, 2013, pp. 2047–2050.
[68] J. K. Butler Jr, Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory, Journal of management 17 (3) (1991) 643–663.
[69] B. R. Cha, J. W. Kim, Handling fake multimedia contents threat with collective intelligence in p2p file sharing environments, in: P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2010 International Conference on, IEEE, 2010, pp. 258–263.
[70] M. Tavakolifard, K. C. Almeroth, A Taxonomy to Express Open Challenges in Trust and Reputation Systems, Journal of Communications 7 (7) (2012) 538–551.
[71] ISO/IEC 27010:2015 Information Technology – Security Techniques – Informa-

tion Security Management for Inter-Sector and Inter-Organizational Communications, http://www.iso27001security.com/html/27010.html, Accessed on: 2017-04-04 (2015).
[72] S. Nusrat, J. Vassileva, Recommending services in a trust-based decentralized user modeling system, in: International Conference on User Modeling, Adaptation, and Personalization, Springer, 2011, pp. 230–242.
[73] P. Resnick, R. Zeckhauser, Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system, in: The Economics of the Internet and E-commerce, Emerald Group Publishing Limited, 2002, pp. 127–157.
[74] W. Rao, L. Chen, P. Hui, S. Tarkoma, Move: A large scale keyword-based content filtering and dissemination system, in: Distributed Computing Systems (ICDCS), 2012 IEEE 32nd International Conference on, IEEE, 2012, pp. 445–454.
[75] T. A. Almeida, A. Yamakami, Content-based spam filtering, in: Neural Networks (IJCNN), The 2010 International Joint Conference on, IEEE, 2010, pp. 1–7.
[76] C. Dong, A. Agarwal, A relevant content filtering based framework for data stream summarization, in: International Conference on Social Informatics, Springer, 2016, pp. 194–209.
[77] M. Vanetti, E. Binaghi, B. Carminati, M. Carullo, E. Ferrari, Content-based filtering in on-line social networks, in: International Workshop on Privacy and Security Issues in Data Mining and Machine Learning, Springer, 2010, pp. 127–140.
[78] C. Tryfonopoulos, S. Idreos, M. Koubarakis, P. Raftopoulou, Distributed large-scale information filtering, in: Transactions on Large-Scale Data-and Knowledge-Centered Systems XIII, Springer, 2014, pp. 91–122.
[79] S. Mittal, P. K. Das, V. Mulwad, A. Joshi, T. Finin, Cybertwitter: Using twitter to generate alerts for cybersecurity threats and vulnerabilities, in: Advances in Social Networks Analysis and Mining (ASONAM), 2016 IEEE/ACM International Conference on, IEEE, 2016, pp. 860–867.
[80] L. Sweeney, k-anonymity: A model for protecting privacy, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10 (5) (2002) 557–570.
[81] A. Machanavajjhala, D. Kifer, J. Gehrke, M. Venkitasubramaniam, *L*-diversity: Privacy beyond *k*-anonymity, TKDD 1 (1) (2007) 3.
[82] N. Li, T. Li, S. Venkatasubramanian, t-closeness: Privacy beyond k-anonymity and l-diversity, in: Proceedings of the 23rd International Conference on Data Engineering, ICDE 2007, The Marmara Hotel, Istanbul, Turkey, April 15-20, 2007, 2007, pp. 106–115.
[83] C. Dwork, Differential privacy: A survey of results, in: International Conference on Theory and Applications of Models of Computation, Springer, 2008, pp. 1–19.
[84] J. Biskup, U. Flegel, On pseudonymization of audit data for intrusion detection, in: Designing Privacy Enhancing Technologies, Springer, 2001, pp. 161–180.
[85] B. Riedl, T. Neubauer, G. Goluch, O. Boehm, G. Reinauer, A. Krumboeck, A secure architecture for the pseudonymization of medical data, in: Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on, IEEE, 2007, pp. 318–324.
[86] T. Neubauer, J. Heurix, A methodology for the pseudonymization of medical data, International journal of medical informatics 80 (3) (2011) 190–204.
[87] J. M. de Fuentes, L. González-Manzano, J. Tapiador, P. Peris-Lopez, PRACIS: Privacy-Preserving and Aggregatable Cybersecurity Information Sharing, Computers & Security.
[88] D. M. Best, J. Bhatia, E. S. Peterson, T. D. Breaux, Improved cyber threat indicator sharing by scoring privacy risk, in: Technologies for Homeland Security (HST), 2017 IEEE International Symposium on, IEEE, 2017, pp. 1–5.
[89] C. Johnson, L. Badger, D. Waltermire, J. Snyder, C. Skorupka, Guide to Cyber Threat Information Sharing, NIST Special Publication 800 (2016) 150.
[90] B. Applebaum, H. Ringberg, M. J. Freedman, M. Caesar, J. Rexford, Collaborative, privacy-preserving data aggregation at scale, in: International Symposium on Privacy Enhancing Technologies Symposium, Springer, 2010, pp. 56–74.
[91] J. Xu, J. Fan, M. H. Ammar, S. B. Moon, Prefix-preserving ip address anonymization: Measurement-

based security evaluation and a new cryptography-based scheme, in: Network Protocols, 2002. Proceedings. 10th IEEE International Conference on, IEEE, 2002, pp. 280–289.

[92] L. Dandurand, A. Kaplan, P. Kacha, Y. Kadobayashi, A. Kompanek, T. Lima, T. Millar, J. Nazario, R. Perlotto, W. Young, Standards and tools for exchange and processing of actionable information, Tech. rep. (2014).

[93] M. Janssen, Y.-H. Tan, Dynamic capabilities for information sharing: Xbrl enabling business-to-government information exchange, in: System Sciences (HICSS), 2014 47th Hawaii International Conference on, IEEE, 2014, pp. 2104–2113.

[94] G. Fisk, C. Ardi, N. Pickett, J. Heidemann, M. Fisk, C. Papadopoulos, Privacy principles for sharing cyber security data, in: 2015 IEEE Symposium on Security and Privacy Workshops, SPW 2015, San Jose, CA, USA, May 21-22, 2015, 2015, pp. 193–197.

[95] O. Serrano, L. Dandurand, S. Brown, On the design of a cyber security data sharing system, in: Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security, ACM, 2014, pp. 61–69.

[96] F. Martinelli, I. Matteucci, M. Petrocchi, L. Wiegand, A formal support for collaborative data sharing, in: International Conference on Availability, Reliability, and Security, Springer, 2012, pp. 547–561.

[97] S. Dietrich, J. Van Der Ham, A. Pras, R. van Rijswijk Deij, D. Shou, A. Sperotto, A. Van Wynsberghe, L. D. Zuck, Ethics in data sharing: developing a model for best practice, in: Security and Privacy Workshops (SPW), 2014 IEEE, IEEE, 2014, pp. 5–9.

[98] E. A. Fischer, E. C. Liu, J. Rollins, C. A. Theohary, The 2013 cybersecurity executive order: Overview and considerations for congress, Congressional Research Service (2013) 7–5700.

[99] F. Skopik, G. Settanni, R. Fiedler, A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing, Computers & Security 60 (2016) 154–176.

[100] A. Schwartz, S. C. Shah, M. H. MacKenzie, S. Thomas, T. S. Potashnik, B. Law, Automatic threat sharing: How companies can best ensure liability protection when sharing cyber threat information with other companies or organizations, U. Mich. JL Reform 50 (2016) 887.

[101] J. Bhatia, T. D. Breaux, L. Friedberg, H. Hibshi, D. Smullen, Privacy risk in cybersecurity data sharing, in: Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, ACM, 2016, pp. 57–64.

[102] C. Sullivan, E. Burger, in the public interest: The privacy implications of international business-to-business sharing of cyber-threat intelligence, Computer Law & Security Review 33 (1) (2017) 14–29.