2020 12th International Conference on Cyber Conflict
20/20 Vision: The Next Decade
T. Jančárková, L. Lindström,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2020 © NATO CCDCOE Publications, Tallinn

Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection

Livinus Obiora Nweke
Information Security and
Communication Technology
Norwegian University of Science and
Technology (NTNU)
Gjøvik, Norway
livinus.nweke@ntnu.no

Stephen Wolthusen
School of Mathematics and
Information Security
Royal Holloway, University of London
Egham, United Kingdom
stephen.wolthusen@rhul.ac.uk
Information Security and
Communication Technology
Norwegian University of Science and
Technology (NTNU)
Gjøvik, Norway
stephen.wolthusen@ntnu.no

Abstract: The menace of cyber attacks has become a concern for both the public and private sectors. Several approaches have been proposed to tackle the challenge, but an approach that has received widespread acceptance among cyber security professionals in both public and private sectors is cyber threat information (CTI) sharing. CTI refers to any information that can help an organisation identify, assess, monitor and respond to cyber threats. It includes indicators of compromise; tactics, techniques and procedures used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents. Sharing CTI has been proposed as an efficient and effective way of improving overall cyber intelligence and defence. However, there are sources of liability that may dissuade private entities from participating in such sharing. The most cited source of liability is privacy and data protection law; although antitrust law, tort of negligence law and intellectual property law are also

cited as potential sources of liability. In this study, we review the extent to which the provisions of privacy and data protection law support or refute the sharing of CTI. This will provide guidance and incentives for private entities willing to participate in CTI sharing, especially for critical infrastructure protection.

Keywords: *legal issues, CTI sharing, GDPR, critical infrastructure protection*

1. INTRODUCTION

In recent years, the cost of cyber incidents has been rising. The Internet Society's Online Trust Alliance (OTA) reports that more than 2 million cyber incidents occurred in 2018, resulting in over $45 billion in losses.[1] The report notes that the financial impact of ransomware rose by 60%, losses from business email compromise doubled and crypto-jacking incidents more than tripled. Attacks on critical infrastructure are also expected to rise. For instance, the Department of Homeland Security in the United States (US) observes that 54% in the utility sector expect a cyber attack on critical infrastructure in 2020.[2] Considering the complexities in the cyber threat landscape, organisations can no longer rely on internally generated cyber threat intelligence (CTI) to protect themselves against these rising threats. Thus, CTI sharing has been proposed as an efficient and effective way of improving overall cyber intelligence and defence.

CTI sharing involves exchanging information relating to threat intelligence between entities, usually of a similar nature, for the purpose of enhancing their security posture by exploiting their collective knowledge, experience and capabilities.[3] Several studies have shown that CTI sharing is an effective tool for organisations to protect themselves against cyber attacks.[4] It enables organisations to understand trending cyber attacks and to implement the most efficient and effective strategies in combating those attacks.

1 Internet Society's Online Trust Alliance (OTA), '2018 cyber incident & breach trends report' (OTA, 9 July 2019) <https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf> accessed 11 December 2019.

2 Homeland Security Today, '54 Percent in Utility Sector Expect Cyber Attack on Critical Infrastructure in Next Year' (Homeland Security Today, 8 October 2019) <https://www.hstoday.us/subject-matter-areas/infrastructure-security/54-percent-in-utility-sector-expect-cyber-attack-on-critical-infrastructure-in-next-year/> accessed 16 December 2019.

3 National Institute of Standards and Technology (NIST), *Guide to Cyber Threat Information Sharing* (NIST Special Publication 800-150 2016) iii.

4 Cristin Goodwin and J. Paul Nicholas, *A Framework for Cybersecurity Information Sharing and Risk Reduction* (Microsoft 2015) 3.

There are several contexts in which CTI can be shared. It can be from a government to another government or to private entities; private entities sharing CTI with each other; or when private entities share CTI in their possession with the government.[5] In this paper, we examine CTI sharing in the context of private entities sharing cyber intelligence with each other: for example, when several companies in a sector (for example, the critical infrastructure sector) establish a formal exchange or formal agreements to share relevant CTI.[6] Such sharing frameworks would enable private entities to leverage the shared knowledge and techniques to better protect their assets while assisting others to do the same.

Private entities that wish to share CTI in their possession with others are faced with legal questions and would have to consider if any information they intend to share contains material that is potentially protected under data protection and privacy law, antitrust law, tort of negligence law, or intellectual property law. We focus on data protection and privacy law as it has shown to be the source of greatest concern, discouraging private entities willing to participate in CTI sharing. We consider the provisions of laws and regulations in the European Union (EU), Norway and the US related to CTI sharing, as those in the US and EU are models for many jurisdictions around the world.

In this paper, we first present the basic concepts of CTI sharing, including the existing CTI sharing architectures, benefits and challenges. We then provide a survey of the existing laws and regulations, which will serve as the basis for providing guidance and incentives for private entities willing to participate in CTI sharing. Lastly, we present a discussion on how well the existing laws and regulations address the concerns of private entities that are willing to participate in CTI sharing with each other. By reviewing the extent to which the provisions of the laws and regulations support or refute the sharing of CTI, we hope to provide guidance and incentives for private entities willing to participate in CTI sharing, especially for critical infrastructure protection.

The rest of this paper is organised as follows. Section 2 presents basic CTI sharing concepts including the existing CTI sharing architectures, the benefits and the challenges. Section 3 provides a survey of laws and regulations in the EU, Norway and the US related to CTI sharing; it also discusses the current trends among practitioners related to the legal implications of CTI sharing among private entities. Section 4 presents a discussion of how well the existing laws and regulations address the concerns of private entities willing to participate in CTI sharing. Section 5 concludes the paper and suggests future work.

5 Andrew Nolan, *Cybersecurity and Information Sharing: Legal Challenges and Solutions* (Congressional Research Service 2015) 5.

6 Ibid. 6.

2. BACKGROUND

In this section, we present basic CTI sharing concepts including the existing CTI sharing architectures. We also explore the benefits and challenges to provide the necessary background for an understanding of the legal issues related to CTI sharing among private entities.

A. Existing CTI Sharing Architectures

CTI refers to any information that can help an organisation identify, assess, monitor and respond to cyber threats. It includes indicators of compromise; the tactics, techniques and procedures (TTPs) used by threat actors; suggested actions to detect, contain or prevent attacks; and the findings from the analysis of incidents.[7] It is no longer the case that organisations must rely only on internal threat intelligence for protection from ever-evolving cyber threats. Hence, the sharing of CTI between entities usually of a similar nature has been proposed as an efficient and effective approach for addressing the complexities of the cyber threat landscape.

Two basic CTI sharing architectures may be adopted by private entities willing to share CTI. The first approach is the use of a centralised architecture, where a central organisation is responsible for the exchange of CTI among the participating entities and may have to perform additional processing to enrich the information.[8] The central body ensures interoperability by using open, standard data formats and transport protocols to provide timely and seamless portability of CTI. Typical examples of centralised architecture are the Information Sharing and Analysis Centres (ISACs).

ISACs provide a central resource for collecting information on cyber threats (in many cases relating to critical infrastructure) and facilitate active sharing of information between the private and the public sectors.[9] They are usually trusted entities that are constituted by representatives of critical infrastructure owners and operators. ISACs were originally created in the US after the first terrorist attacks on the World Trade Centre. The main objective was to identify opportunities for cooperation between the public and private sectors for the protection of US critical infrastructure.[10] European legislation also advocates cooperation in cybersecurity which the creation of ISACs represents. For example, the NIS Directive encourages incident reporting and the sharing of information with computer security incident response teams (CSIRTs) which involves the sharing of threat intelligence.[11]

7 National Institute of Standards and Technology (NIST), *Guide to Cyber Threat Information Sharing* (NIST Special Publication 800-150 2016) ii.
8 Ibid. 17.
9 European Union Agency for Network and Information Security (ENISA), *ENISA'S Opinion Paper on ISAC Cooperation* (Opinion Paper 2019) 3.
10 Ibid. 3.
11 Ibid. 4.

The second CTI sharing architecture is the peer-to-peer architecture, where private entities that are willing to share CTI with each other do so directly without an intermediary. This type of architecture enables great agility in that participants can receive CTI directly from the source and the problem of having a single point of failure as in the case of centralised architecture is eliminated.[12] A typical example of a peer-to-peer architecture of CTI sharing can be found in the power sector.[13]

Regardless of which CTI sharing architecture an organisation decides to adopt, there is a need to establish information sharing rules before proceeding. The NIST guide to CTI sharing recommends the following rules:[14]

- List the types of threat information that may be shared.
- Describe the conditions and circumstances when sharing is permitted.
- Identify approved recipients of threat information.
- Describe any requirements for redacting or sanitising information to be shared.
- Specify if source attribution is permitted.
- Apply information handling designations that describe recipient obligations for protecting information.

These rules would help to ensure that the publication and dissemination of threat information are controlled. The goal is to prevent the sharing of information that, if not properly handled, may have serious legal implications for the organisation.[15]

However, these rules are not quite complete as far as NIST provides. Specifically, the issue of sanitising information is unfortunately not something that can be solved based on a single record. With multiple anonymised records or queries, it will be possible to de-anonymise or otherwise fill in the gaps of queries. So, one has to either accept that sanitising offers only a weak form of anonymity and prevention of leaking sensitive information or has to use far more restrictive measures.

B. Benefits of CTI Sharing

CTI sharing provides organisations with access to threat information that ordinarily they may not have been able to obtain without participating in such a sharing endeavour. Organisations can exploit these shared resources to improve their overall security

12 National Institute of Standards and Technology (NIST), *Guide to Cyber Threat Information Sharing* (NIST Special Publication 800-150 2016) 17.

13 Steve Livingston, Suzanna Sanborn, Andrew Slaughter and Paul Zonneveld, 'Managing Cyber Risk in the Electric Power Sector: Emerging Threats to Supply Chain and Industrial Control Systems' (Deloitte Insights, 2018) <https://www2.deloitte.com/content/dam/insights/us/articles/4921_Managing-cyber-risk-Electric-energy/DI_Managing-cyber-risk.pdf> accessed 11 April 2020.

14 National Institute of Standards and Technology (NIST), *Guide to Cyber Threat Information Sharing* (NIST Special Publication 800-150 2016) 10.

15 Ibid. 5.

posture by using the knowledge, experience and capabilities of the participating entities. This ensures that the detection of one organisation becomes the prevention of another.[16]

There are several ways that an organisation can use the shared threat information. It might use the information for operational purposes, such as updating its security controls for continuous monitoring with new indicators and configurations to detect the latest attacks and comprises.[17] The shared threat information might also be used strategically, such as when planning major changes to an organisation's security structure.[18]

Sharing CTI between entities of a similar nature can be greatly beneficial because participating entities will often face actors that use similar TTPs and target the same types of infrastructures. Defending against cyber threats is much more effective and efficient when organisations collaborate to defend against well-organised and capable actors.[19] This type of alliance will enable organisations to mitigate risks and ameliorate their overall security readiness.

The additional benefits of CTI sharing have been identified as including the following: shared situational awareness, where organisations exploit the collective knowledge, experience and analytical capabilities of the participating entities; improved security posture, which allows organisations to implement protective measures, improve detection capabilities and more effectively respond to and recover from incidents based on observed trends in the threat landscape; knowledge maturation, which enriches the value of threat information; and greater defensive agility, where participating entities adapt quickly to evolving threats.[20] Whilst there are benefits in CTI sharing, it still poses some challenges that need to be considered, some of which are explored in the following subsection.

C. Challenges of CTI Sharing

One of the prerequisites to CTI sharing involves establishing a trust relationship among the participating entities.[21] This process can be very challenging, as building trust requires a lot of work to develop and sustain it. However, an organisation's ability to establish trust between entities willing to share CTI is pivotal to the success of any CTI sharing scheme. Hence, the cost and effort required to build a trust relationship

16 Ibid. 3.
17 Cristin Goodwin and J. Paul Nicholas, *A framework for cybersecurity information sharing and risk reduction* (Microsoft 2015) 10.
18 National Institute of Standards and Technology (NIST), *Guide to Cyber Threat Information Sharing* (NIST Special Publication 800-150 2016) 3.
19 Ibid. 3.
20 Ibid. 3-4.
21 Cristin Goodwin and J. Paul Nicholas, *A framework for cybersecurity information sharing and risk reduction* (Microsoft 2015) 3.

among participating entities may discourage an organisation's willingness to join in such a sharing scheme.

Achieving interoperability and automation have also been cited as challenges to CTI sharing.[22] The problem of interoperability seems to be more profound for organisations that adopt peer-to-peer sharing architecture than for those that choose centralised architecture. However, both types of sharing architectures must deal with the additional complexities introduced by automation. With the use of automation, the participating entities would have to agree on the data format and methodology to be employed. All these require organisations to invest additional resources in ensuring that the shared CTI can be automated and be easily reusable by the participating entities.

Organisations participating in CTI sharing may not want to disclose their identity to avoid a perceived risk to the organisation's reputation. The unwillingness to disclose their identity could be problematic as the credibility of the shared threat information may be brought into disrepute.Also, it is natural for participating entities to doubt the credibility of shared information if its source is unknown. Therefore, organisations willing to participate in CTI sharing may have to weigh the perceived risk to the reputation of the organisation against the dangers of not sharing threat information.

Another challenge that may discourage private entities from participating is the problem of incomplete or false information. This means that there is the possibility of any of the participating parties sharing incomplete or false information which may contaminate or mislead the algorithms or analysts. In such a scenario, the danger is that it either disincentivises sharing or encourages other participating entities to share questionable information. Any liability waiver usually becomes void when negligence is involved, so there are some data quality obligations inherent in CTI sharing arrangements that must be considered.

Legal liability that may arise from CTI sharing is a major source of concern for organisations willing to participate in such sharing schemes.[23] This is because the legal issues relating to CTI sharing tend to be complex and they have very few certain resolutions.[24] Various laws and regulations have been proposed and implemented to address such concerns. For example, the Cybersecurity Information Sharing Act (CISA) was approved by the US Congress in 2015 to provide legal protection for organisations that participate in CTI sharing. In Europe, a similar cybersecurity framework offers the same protection against any liability that may result from CTI

22 National Institute of Standards and Technology (NIST), *Guide to Cyber Threat Information Sharing* (NIST Special Publication 800-150 2016) 4.

23 Andrew Nolan, *Cybersecurity and Information Sharing: Legal Challenges and Solutions* (Congressional Research Service 2015) 5.

24 Ibid.

sharing for the protection of network and information systems across the Union.[25] These legal protections require organisations to follow set rules when sharing CTI. The next section provides a review of these laws and regulations to assess the extent to which they support or refute the sharing of CTI among private entities.

3. LAWS AND REGULATIONS RELATED TO CTI SHARING

Various laws and regulations have been proposed to encourage CTI sharing and we provide a survey of these laws and regulations in this section. The purpose of this review is to assess their provisions, which will then serve as the basis for providing guidance and incentives for private entities willing to engage in CTI sharing.

A. Laws and Regulations in the European Union (EU)

A good number of laws and regulations have been proposed in the EU over the years to promote the sharing of CTI. The most relevant of these are Directive (EU) 2016/1148 of 6 July 2016,[26] also known as the network and information systems (NIS) Directive; the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 of 27 April 2016);[27] and the EU Cybersecurity Act (Regulation (EU) 2019/881 of 17 April 2019).[28] In the EU, a Regulation is a binding legislative act that is directly applicable in its entirety across the EU; while a Directive is a legislative act that stipulates goals that all EU countries must achieve (minimum-level legal provisions), but it is incumbent on the individual countries to promulgate their own laws in order to reach these goals.[29]

The NIS Directive can be considered the first EU-wide cybersecurity legislation. It aims to enhance cybersecurity across the EU. The directive encourages the sharing of CTI for the protection of critical infrastructure by providing an enabling environment for setting up ISACs which will foster the sharing CTI within and between the EU member states. Following the adoption of the NIS directive in 2016, it became an EU

25 Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, 'The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation' (2019) 35(6) Computer Law and Security Review <https://www.sciencedirect.com/science/article/pii/S0267364919300512> accessed 12 April 2020.

26 Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1.

27 Regulation (EU) 2016/679 on the protection of natural persons with regards to the processing of personal data and on free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

28 Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15.

29 European Union, 'Regulations, Directives and other acts' (EU Law, 7 March 2019) < https://europa.eu/european-union/eu-law/legal-acts_en> accessed 20 December 2019.

Directive requiring that every member state adopt national legislation which follows or 'transposes' the directive.[30] In general, the NIS Directive has three main parts:[31]

- **National capabilities:** EU member states must have certain national cybersecurity capabilities such as a national CSIRT and must perform cyber exercises, etc.
- **Cross-border collaboration:** Cross-border collaboration between EU countries, including the operational EU CSIRT network and the strategic NIS cooperation group.
- **National supervision of critical sectors:** EU member states must supervise the cybersecurity of critical market operators in their country: ex-ante supervision in critical sectors (energy, transport, water, health and finance), ex-post supervision for critical digital service providers (internet exchange points, domain name systems, etc).

The NIS Directive observes that the 'responsibilities in ensuring the security of network and information systems lie, to a great extent, with operators of essential services'.[32] It does differentiate between sectors, placing higher burdens on critical infrastructure operators. The implication of this is that private entities that provide essential services (critical infrastructure operators) are obliged to ensure the protection of their network and information systems. The NIS Directive encourages a culture of risk management, which include risk assessment and the implementation of appropriate security measures for the protection of network and information systems within the critical infrastructure sector. Among these measures is the sharing of CTI.

Regulation (EU) 2016/679,[33] or GDPR as it is better known, has been hailed as the model for data protection and privacy laws both in Europe and beyond.[34] The goal of the Regulation is to harmonise data and privacy laws across Europe, to increase the levels of protection for EU citizens and to give them greater control over their personal data. The regulation 'protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'.[35] It has also redefined the way organisations across Europe and how those who offer goods and/or services to EU citizens around the globe, process personal data. GDPR contains provisions and requirements that are related to the processing of personal data of individuals

30 Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1.
31 Ibid.
32 Ibid.
33 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
34 Clare Sillivan and Eric Burger, '"In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence' (2017) 33(1) Computer Law and Security <https://www.sciencedirect.com/science/article/pii/S0267364916302229> accessed 21 December 2019.
35 Regulation (EU) 2016/679 Art 1.

(data subjects) inside the European Economic Area (EEA). These provisions and requirements include the provisions that cover the scope, application and objectives of the data protection regulations and the implementing arrangements.

The EU Cybersecurity Act's main objective is to provide a permanent mandate for the ENISA and to establish a cybersecurity certification framework. It strengthens ENISA through the provision of more resources and a legal framework to improve cybersecurity capabilities at Union level, among member states, Union institutions, bodies, offices and agencies and relevant private and public stakeholders on matters related to cybersecurity.[36] Among the provisions of the EU Cybersecurity Act, the provision that is most relevant to this study is Article 6(2), which states that 'ENISA shall support information sharing in and between sectors, in particular in the sectors listed in Annex II to Directive (EU) 2016/1148, by providing best practices and guidance on available tools and procedures, as well as on how to address regulatory issues related to information-sharing'.[37]

B. Laws and Regulations in Norway and the US

In this subsection, we examine the laws and regulations in Norway and the US to review efforts in other countries outside the EU regarding CTI sharing. Norway is a member of the European Economic Area (EEA) and so some EU regulations are also applicable. Like other EEA member states, Norway is required to promulgate laws in line with EU Directives if they are relevant to the EEA. The Norwegian National Security Act (Security Act) is the most relevant law in Norway to this study. In the US, the Cybersecurity Information Sharing Act of 2015 (CISA) is considered to be the most significant cyber-related legislation as it establishes a mechanism for cybersecurity information sharing among private sector and government entities.[38] CISA has greatly impacted the sharing of CTI not just in the US but also around the world; thus, deserves consideration.

The Security Act took effect on January 1, 2019. Its purpose is threefold: to safeguard Norway's sovereignty, territorial integrity and democratic governance and other national security interests; to prevent, detect and counteract security threats; and to ensure that security measures are implemented in accordance with basic legal principles and values in a democratic society.[39] It is mainly concerned with security-rated information, information systems and objects or infrastructure essential for basic national functions (critical infrastructure). It applies to state, county and municipal bodies and to suppliers of goods or services that can access or produce security-classified information.[40] For example, Article 2(3) requires that 'the security

36 Ibid.
37 Ibid. Art 6.
38 John Heidenreich, 'The Privacy Issues Presented by the Cybersecurity Information Sharing Act' (2015) 91(395) North Dakota Law Review < https://law.und.edu/_files/docs/ndlr/pdf/issues/91/2/91ndlr395.pdf> accessed 21 December 2019.
39 National Security Act (Norway) LOV-2018-06-01-24 (Security Act) [2018] Jnr 2018-0165 ch 1, art 1.
40 Ibid. ch 1, art 2-3.

authority shall ensure that businesses to which the law applies will have access to information on threat assessments and other information that is important for the companies' preventive security work'.[41] This implies that the Act not only supports an organisation's monitoring of its information systems to prevent, detect and counteract cyber incidents, it also offers greater flexibility to organisations when implementing such security measures including CTI sharing.

CISA was signed into law on December 18, 2015. The law has two main components: it authorises companies to monitor and implement defensive measures on their own information systems to counter cyber threats and it provides certain protections to encourage companies to share CTI.[42] Title I of the law is of greatest interest to private sector bodies willing to participate in cyber threat intelligence sharing. It states that 'non-federal entities can share CTI among themselves and with federal departments and agencies'.[43] It provides several safeguards which include protection from liability, non-waiver privilege and protection from Freedom of Information Act (FOIA) disclosure. Organisations that are covered by these protections must comply with CISA's requirements when participating in CTI sharing.

C. Legal Implications of CTI Sharing

We have provided a survey of the existing laws and regulations in the EU, Norway and the US related to CTI sharing. Our focus in this paper is on provisions that are related to personal data protection. A general theme of these laws and regulations is that CTI sharing is lawful but that care should be taken not to share information protected by data protection and privacy laws. In addition to the survey presented in the preceding section, we provide a discussion on the current trends among practitioners related to the legal implications of CTI sharing among private entities in this subsection.

Many authors have considered the extent to which the provisions of GDPR affect CTI sharing. Article 4(1) defines personal data as:

> 'any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.[44]

41 Ibid. ch 2, art 3.

42 S.754 An Act to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes (Cybersecurity Information Sharing Act of 2015) [2015].

43 Ibid.

44 Regulation (EU) 2016/679 on the protection of natural persons with regards to the processing of personal data and on free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, art 4.

CTI is likely to contain sensitive and identifying information such as IP and email addresses.[45] This may raise concerns for private entities willing to participate in CTI sharing as they must ensure conformance with legal and regulatory requirements.

Borden et al. have argued that CTI sharing is lawful under GDPR.[46] They observe that the provision of Article 6, which requires 'legitimate interests' for the processing of personal data in CTI, is satisfied by private entities participating in such a scheme. They also suggest that GPDR Recitals 47, 49 and 50 supports the processing of personal data for fraud prevention, ensuring network and information security and indicating possible acts or threats to public security. These are all goals of CTI sharing.

Sullivan and Burger discuss the legal issues related to international business-to-business sharing of cyber threat intelligence.[47] They opine that data protection and privacy laws affect the willingness of private entities to participate in CTI sharing. They use GDPR as a case study (considering that its requirements do not only apply to companies incorporated in the EU but also to third countries and international organisations) to investigate whether automated sharing of information between businesses may be legal. The study concludes that the sharing of cyber threat intelligence between businesses is likely to be necessary for the legitimate interests of the data controller under Article 6(1)(f) of GDPR and may be clearly justified and lawful on public interest grounds.

Similarly, Maltzan observes that Article 6(1)(f) of GDPR may be used as a legal ground for the processing of personal data when private entities participate in sharing of CTI with each other.[48] She maintains in the paper that the legitimate interest clause may allow the data controller to process personal data if none of the other circumstances listed in Article 6 of GDPR will suffice as a legal basis. She also notes that the lawfulness of CTI sharing under the provision requires an assessment of the test for validity based on the legitimacy and necessity of the processing and balance between the interests of the data controller and data subject. According to the Article 29 Working Party, 'this balance of interest test should consider issues of proportionality,

45 Adham Albakri, Eerke Boiten and Rogério De Lemos, 'Risks of Sharing Cyber Incident Information' In Proceedings of International Conference on Availability, Reliability and Security, Hamburg, Germany, August 27–30 2018 (ARES 2018) <https://dl.acm.org/doi/pdf/10.1145/3230833.3233284> accessed 18 December 2019.

46 Richard Borden, Joshua Mooney, Mark Taylor, and Matthew Sharkey, 'Threat Information Sharing Under GDPR' (American Bar Association, 6 March 2019) <https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2019/spring/threat-information-sharing-under-gdpr/> accessed 20 December 2019.

47 Clare Sullivan and Eric Burger, ''In the public interest': The privacy implications of international business-to-business sharing of cyber-threat intelligence' (2017) 33(1) Computer Law and Security <https://www.sciencedirect.com/science/article/pii/S0267364916302229> accessed 21 December 2019.

48 Stephanie Von Maltzan, 'No contradiction between cyber-security and data protection? designing a data protection compliant incident response system' (2019) 10(1) EJLT <http://ejlt.org/article/view/665/893> accessed 22 December 2019.

the relevance of the personal data to the litigation and the consequences for the data subject'.[49]

Although our focus in this paper is on provisions related to personal data protection, other concerns may discourage private entities from participating in CTI sharing. Private entities that wish to share CTI may also have to consider if any of the information they intend to share contains material that is potentially protected under antitrust law, tort of negligence law or intellectual property law.[50] The laws and regulations that we have reviewed in this paper protect from liability for private entities only as long as they conform with the laid down requirements when sharing CTI, including removal of personal data that may be found in it. For example, the US Department of Justice released a statement clearly noting that CTI sharing does not raise antitrust issues.[51] It observes that private entities that participate in such sharing activities do not violate antitrust laws as the shared information is very technical in nature and very different from the sharing of competitively sensitive information such as current or future prices and output or business plan.

In general, the greatest concern for private entities willing to participate in CTI sharing is to consider whether any of the information they intend to share contains material that is protected by data protection and privacy laws. However, processing of CTI and subsequent sharing with others for the protection of network infrastructure can be viewed as 'legitimate interests'. Therefore, in agreement with the studies discussed above, we note that Article 6(1)(f) of GDPR may be used as the legal basis for private entities to participate in sharing CTI and that the principles stated in Article 5 of GDPR still need to be observed.

4. DISCUSSION

In this section, we present a discussion on how well the existing laws and regulations address the concerns of private entities willing to participate in CTI sharing with each other. Ambiguity in laws and regulations often breeds litigation and the costs of litigation may be significant enough to deter private entities from engaging in CTI sharing. This section considers whether there are legal and regulatory requirements that make the identified concerns difficult to address.

49 Article 29 Data Protection Working Party WP 136 Opinion 4/2007 on the concept of personal data [2007] 01248/07/EN.

50 Andrew Nolan, Cybersecurity and Information Sharing: Legal Challenges and Solutions (Congressional Research Service 2015) 12.

51 Department of Justice and Federal Trade Commission, Antitrust Policy Statement on Sharing of Cybersecurity Information (Policy Statement, United States Department of Justice and Federal Trade Commission) [2014].

There is a consensus among the existing laws and regulations and the current discussion among practitioners that cyber threat sharing can be performed lawfully. However, organisations that wish to participate in CTI sharing among themselves would have to consider issues that could arise from the disclosure of personal information, breaches of contractual terms and disclosure of sensitive or classified information. For example, CISA offers several safeguards for private entities that participate in CTI sharing, which include protections from liability, non-waiver privilege and protections from FOIA disclosure.[52] These protections are likely to become void when negligence leads to the disclosure of personal information, breaches of contractual terms or disclosure of classified information.

Organisations must take care when sharing CTI containing personal information. However, when such sharing becomes necessary, Article 6(1)(f) of GDPR may serve as a legal basis. CTI containing personal data also raises additional concerns for automating the CTI sharing process. This requires private entities to invest additional resources. They may also have to consider the likelihood of the shared information containing personal information. Articles 25 and 32 of GDPR offer suggestions on how to implement technical and organisational measures to mitigate the risks associated with processing such data.[53] Organisations may have to examine how these technical and organisational measures can be included when deploying an automated CTI sharing system.

Another issue likely to make the legal and regulatory requirements difficult to address is the civil liability that may arise from breaches of contractual terms. For example, if a company were to give its trade secrets as part of a CTI exchange, this might expose its directors to civil liability. The disclosure of sensitive or classified information could make the legal and regulatory requirements that cause the identified concerns difficult to address, because such information may cause serious injury to the national interest.

It would also be interesting to investigate how the decision-making process can be supported in private entities. This will enable them to share CTI in compliance with existing laws and regulations. Albakri, Boiten and Lemos have presented a model for evaluating the legal requirements for supporting decision-making when sharing CTI in the context of GDPR.[54] They describe the effect that GDPR legal aspects may have on the sharing of CTI and have translated the existing legal provisions into

52 S.754 An Act to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes (Cybersecurity Information Sharing Act of 2015) [2015].

53 Regulation (EU) 2016/679 on the protection of natural persons with regards to the processing of personal data and on free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

54 Adham Albakri, Eerke Boiten and Rogério De Lemos, 'Sharing Cyber Threat Intelligence Under the General Data Protection Regulation' In: Naldi, M., Italiano, G.F., Rannenberg, K., Medina, M., Bourka, A. (eds.) *Privacy Technologies and Policy - 7th Annual Privacy Forum*, APF 2019, Rome, Italy, June 13-14, 2019, Proceedings. Lecture Notes in Computer Science, vol. 11498, pp. 28–41. Springer (2019) <https://link.springer.com/chapter/10.1007/978-3-030-21752-5_3> accessed 19 December 2019.

rules to enable organisations to share CTI whilst being legally compliant with the requirements for sharing personal information.

However, the work by Albakri et al. can be extended to provide a holistic approach that can guide private entities willing to participate in CTI sharing.[55] The holistic approach for developing such a reference framework would involve extracting the legal requirements from the existing laws and regulations, in addition to the functional and non-functional requirements coming from the CTI sharing architectures. These requirements could then be translated into rules that would guide organisations when they share CTI. This type of framework would allow organisations to demonstrate that they satisfy the legal requirements for CTI sharing and encourage private entities to join such a scheme.

5. CONCLUSIONS

There is no doubt that CTI sharing increases the overall cyber intelligence and defence of organisations. We have conducted a review of existing laws and regulations in the EU, Norway and the US related to CTI sharing. First, we presented the basic concepts of CTI sharing including the existing CTI sharing architectures. We then explored the benefits and challenges of such sharing. We have observed that several laws and regulations have been proposed to encourage CTI sharing among private entities. However, private entities still cite data protection and privacy laws as the greatest concern, discouraging them from participating in CTI sharing.

Our study indicates that the processing of CTI and subsequent sharing with others in a bid to protect network infrastructure and improve overall cyber intelligence and defence can be considered 'legitimate interests' under GDPR for processing of any personal data that may be found in CTI. If none of the other circumstances listed in Article 6 can be invoked as a legal basis, the legitimate interest clause can suffice. Hence, Article 6(1)(f) of GDPR may serve as the legal basis for private entities to participate in CTI sharing, especially for critical infrastructure protection.

Future work will be directed towards considering approaches which organisations can employ to automate the CTI sharing process, and which will still conform with the requirements of existing laws and regulations. For example, Articles 25 and 32 of GDPR offer suggestions on how to implement technical and organisational measures

55 Adham Albakri, Eerke Boiten and Rogério De Lemos, 'Sharing Cyber Threat Intelligence Under the General Data Protection Regulation' In: Naldi, M., Italiano, G.F., Rannenberg, K., Medina, M., Bourka, A. (eds.) *Privacy Technologies and Policy - 7th Annual Privacy Forum*, APF 2019, Rome, Italy, June 13-14, 2019, Proceedings. Lecture Notes in Computer Science, vol. 11498, pp. 28–41. Springer (2019) <https://link.springer.com/chapter/10.1007/978-3-030-21752-5_3> accessed 19 December 2019.

to mitigate the risks associated with the processing of personal data.[56] Thus, it is possible to evaluate these legal requirements for automating CTI sharing to translate the existing legal provisions into rules that will enable organisations to share CTI whilst being legally compliant.

56 Regulation (EU) 2016/679 on the protection of natural persons with regards to the processing of personal data and on free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, art 25, 32.