CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELL

Whole-of-Government Cyber Information Sharing

İhsan Burak Tolga
NATO CCDCOE Strategy Branch Researcher

Tallinn 2019

About the author

The author İhsan Burak Tolga is a researcher at the CCDCOE Strategy branch.

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 25 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the *Tallinn Manual 2.0*, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise, Locked Shields. Every spring the Centre hosts the International Conference on Cyber Conflict (CyCon), a unique event joining key experts and decision-makers of the global cyber defence community. Since January 2018, CCDCOE has been responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by its member nations; to date Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Spain, Sweden, Turkey, the United Kingdom and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Table of Contents

1. **Introduction** 4
2. The need for cyber information sharing across governmental bodies 5
3. Existing models 7
4. Challenges to cyber information sharing 12
5. Best practices 14
   - 5.1 Acknowledge the actors in the information-sharing environment and define personas 14
   - 5.2 Setting policies and guidelines for information sharing across governmental and civilian bodies 14
   - 5.3 Designating incentives for private organisations to encourage information sharing 14
   - 5.4 Establish an automated framework and formats for rapid information distribution and processing 14
   - 5.5 Designate rules and official regulations for information sharing 15
   - 5.6 Designate and promote shared goals and benefits for organisations regarding information sharing 15
   - 5.7 Set up meetings for overseeing the information sharing process and feedback 15
   - 5.8 Prioritise the information types and areas of importance 16
   - 5.9 Protection of sensitive and classified information 16
   - 5.10 Designate integrity and authenticity levels for shared information 16
   - 5.11 Provide feedback mechanisms for received information 16
6. Conclusion 17

References 18

1. Introduction

Cyberspace, with all its information networks and the residing data at the endpoints of these networks, is expanding very fast.[1] Following the inception of corporate and business networks, personal computers and mobile devices, and now with the emerging Internet of Things (IoT), more information is continuously travelling through global networks. Naturally, there is a direct correlation between the increasing speed of cyber and the associated security and defence risks for its end users and organisations, whether governmental or civilian.

The interconnected networks that make up cyberspace are mostly built and operated by private Internet Service Provider (ISP) companies. In most states, government networks are also a significant part of this cyberspace and in many cases, they are not isolated networks but inter-connected as well. This network of networks includes and enables all the activities and services of the modern world, for which information exchange and use is crucial. For this simple reason, when it comes to security, there is no firm line between private and governmental domains in practice.

Since cyberspace is expanding at an almost exponential rate, the volume of information is also increasing. Besides the recurring data, new and unique information flows into this pool almost every instant. Consequently, the probability of the required information's existence at one or more places in cyberspace at any given time is also getting higher, but this does not necessarily mean that finding the required information is getting easier. Therefore, considering the limited capability of individual organisations, tracking the information in this continuously expanding medium thus requires a cooperative effort among different organizations practicing in cyber.

Since the internet is vast and fully integrated into society, almost all governmental organisations and private companies are in touch with cyber at some point. Considering the operating zone and practice areas of each entity in cyber, they are responsible for different tasks, each one focusing on different aspects of this pool of information. Although they often share a common interest in the information they seek, even while they are not aware of the utility of some of the information in their possession, sometimes that information proves to be valuable to other parties.[2] Potential benefits of cyber information sharing have been always apparent; lowering costs, increasing benefits, wider situational awareness and quick access to data when required. Yet in real life, a complete efficiency and utilization of all information in cyberspace are far from possible.

The paper argues that, even though it is never possible to form such a mechanism for information sharing with flawless efficiency, every effort on the right path will give positive returns. It may help governments to avoid unnecessary duplication of effort in improving their situational awareness and enable the rapid exchange of information. Hence, this paper examines the existing and proposed information sharing frameworks and seeks a set of refined practices along while identifying the associated challenges.

The motivations behind possessing successful information sharing mechanism among governmental bodies are given in the following chapter, after which comes an overview of existing information sharing mechanisms. Moving from existing frameworks, some of the practices of sharing cyber information across government and private bodies, which appeared to be beneficial in the past, are put together later. In addition, the underlying reasons and factors for these practices are provided to assist in the efforts to transform them into policy implications.

---

[1] Stevens, John. 2018. Internet Stats & Facts for 2019. 17 December. Accessed 01 30, 2019. https://hostingfacts.com/internet-facts-stats/.

[2] The White House. 2012. National Strategy for Information Sharing and Safeguarding. Official Strategy Document, Washington: The White House.

2. The need for cyber information sharing across governmental bodies

Cyber threats have become a major factor for nations and their governmental organisations. These threats stem not only from individual hackers or criminal groups, but from other nation states.[3] In 2018, 531 reported major cyber incidents (cyber espionage and cyber warfare, excluding cybercrime) took place against government bodies.[4] In 2017, there were 159,700 successful reported cyber incidents against private business organisations.[5] Reflecting the very rapid increase of cyber incidents, in 2017 global spending on cyber security was predicted to exceed $1 trillion over five years[6] to 2021 with the introduction of IoT products, Industrial Control Systems (ICS) and automotive security.

Cyber attacks take place in instantly, usually without escalation or warnings like conventional counterparts in history. Thus, it is not possible to raise the defending organisations' level of preparedness prior to an attack and there is little opportunity to escalate information sharing level between different bodies after a triggering event. Unlike kinetic attacks in which the source quickly becomes evident, cyber attacks are more difficult to attribute. They typically leave no physical trail and the related cyber forensics tasks are more complicated. As a result, it softens the deterrence postures due to decreased fear in the attackers' mind of any possible consequences. In this case, fast and complete information sharing between different organisations that are defending against similar threats possibly coming from the same source becomes vital to keep the damage on deterrence efforts at a possible minimum.

Defending against such threats and actions in a vast and flexible environment is not an easy task. For most of the time, the main goal for organisations is to facilitate normal operations and business by keeping the information networks available and reliable.

There are often many governmental organisations in individual nations working to defend against cyber-related threats. In some cases, these organisations are dedicated for cyber defence and security missions, such as military Cyber Emergency Response Teams (CERTs), or which are responsible for similar tasks; for instance the CERTs of other government departments or nuclear power plants. Depending on their respective budgets, it is still not possible for them to scan and track all threat information relevant to their specific mission due to the very high volume of information flow and the wide spectrum of information networks for which they are responsible.

Since it is not possible in practice to monitor and scan all the information travelling through relatively big governmental or corporate information networks, neither is it possible to find targeted information regarding the forensics efforts. In that sense, sharing information between organisations enables them to gain access to ones, which used to be outside their capabilities. Hence, they can enhance their knowledge base with new information, enabling even the data pieces that were incoherent before; in some cases, the sum gets even bigger than the addition of the pieces. In this sense, the logic is similar

---

[3] The Wall Street Journal. 2017. The Fight against Nation-State Cyberthreats. 18 December. Accessed January 30, 2019. https://www.wsj.com/articles/the-fight-against-nation-state-cyberthreats-1513653060

[4] Centre for Strategic & International Studies. 2019. *Significant Cyber Incidents.* January. Accessed January 30, 2019. https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

[5] Online Trust Alliance. 2018. *Cyber Incident & Breach Trends Report.* Annual Report, The Internet Society. https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf.

[6] Morgan, Steve. 2017. *Cybersecurity market slowdown? Not anytime soon.* Business Report, CSOOnline. https://www.csoonline.com/article/3242811/security/cybersecurity-market-slowdown-not-anytime-soon.html

to the phrase formulated by Tony Sager: 'One organisation's detection to become another's prevention'[7], promoting the practice of facilitating the required information by classifying and forwarding it to collaborating bodies.

For organisations that maintain an information pool for cyber defence purposes, information received from other entities can be used to validate the existing information. Although it is rather more complicated than is depicted here, particularly with respect to emerging artificial intelligence and machine learning technologies, this is the first step toward evaluating cyber intelligence.

Benefiting from some mediums and domains, which are not accessible under normal conditions due to official restrictions, has never been standard practice in information security. Only in exceptional cases have organisations share required information, and only manually.[8] Although it is logical to restrict the access of outside entities to internal networks and cyber databases, facilitating some controlled flow of information brings extra value to defending one's information networks in cyberspace.

Getting a cyber information feed from a variety of sources also increases situational awareness of the overall organisation cluster. Even in situations where the related information is received from an external source that operates in a different domain, it might be found complementary to existing information, thereby bringing extra value. Besides the value of complementing information, integrating updates might serve useful and enable organisations operating in cyberspace to fix inaccurate points in their datasets.

Sharing information on a robust and seamless level greatly enhances overall cyber deterrence postures of nations. Particularly for nations defending against cyber theft, cyber terrorist groups and common adversaries, the benefit to cost ratio of the information sharing process is promising.

Although it is out of this paper's scope, the partnership between the public and private sector has also been gaining attention recently. Usually, private companies run critical information infrastructure, but states have a responsibility of keeping them functional. Therefore, partnership between the two seems promising for a win-win deal for both ends.

---

[7] Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. 2016. 'Guide to Cyber Threat Information Sharing.' *NIST Special Publication 800-150* 3.

[8] Cristin Goodwin, J. Paul Nicholas. 2015. *A framework for cybersecurity information sharing and risk reduction.* White Paper, Seattle: Microsoft, 15.

3. Existing models

Whereas it is not always particularly about cyber, information sharing across governmental entities has been in place for a long time. Without a universally accepted and proven information exchange model, almost every nation employs a particular mechanism or system of systems to share information across its state bodies with respect to its regulations-in-place regarding the accessibility, authentication, security and speed.

As has been summarised in previous academic work,[9] existing information sharing mechanisms can be studied in two subgroups: privacy-preserving information sharing' and 'non-privacy-preserving information sharing'.

Privacy-preserving information sharing mechanisms are those in which the receiving party or organisation is not handed the raw information or private information about the identity of sending party or organisation. It has three sub-categories.

The first is the trusted third party; in which two entities provide the information they possess to a mutually trusted third party, which processes and mediates the calculated information to the other end. The most crucial thing in this framework is the absolute need for trust in the third party by both entities.

The second is the secure multi-party computation, which seeks to remove the third party from the information flow. In this technique, the parties send and receive the processed information in their and corresponding side's deposit in one of a number of described ways.[10] However, as the number of parties involved in such a scheme increases, the complexity and cost of the information sharing also rise relatively.[11]

The third method is application-specific solutions.[12] As its name suggests, using specific applications, removing the trusted third party from the information flow can be achieved while the involved parties still receive the processed version of the raw information others provide. This process benefits from relational database models and information sharing protocols and can cut the cost of removing the third party from the scheme dramatically.

In the mechanisms under **non-privacy-preserving information sharing**, the parties share the information in whole or in part [13] but attach less importance to privacy concerns.

The first technique is privilege-based information sharing in which the information from a given organisation can be shared on the basis of the roles of each employee.[14] The role here refers to an authorisation, many of which can be possessed by a single employee.[15] Hence, employees with access

---

[9] Peng Liu, Amit Chetal. 2005. 'Trust-based Secure Information Sharing Between Federal Government Agencies.' *Journal of the Association for Information Science and Technology* 6.
[10] Goldreich, Oded. 2002. 'Secure Multi-Party Computation - Draft Version 1.4.' *Department of Computer Science and Applied Mathematics, Weizmann Institute of Science.*
[11] Moni Naor, Kobbi Nissim. 2001. 'Communication Preserving Protocols for Secure Function Evaluation.' *STOC '01 Proceedings of the thirty-third annual ACM symposium on Theory of computing* 590-598.
[12] Agrawal Rakesh, Alexander Evfimievski , Ramakrishnan Srikant. 2003. 'Information sharing across private databases.' *SIGMOD '03 Proceedings of the 2003 ACM SIGMOD international Conference on Management of Data* 86-97.
[13] Peng Liu, Amit Chetal. 2005. 'Trust-based Secure Information Sharing Between Federal Government Agencies.' *Journal of the Association for Information Science and Technology* 6.
[14] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman. 1996. 'Role-Based Access Control Models.' *IEEE Computer, Volume 29, Number 2* 38-47
[15] Longhua Zhang, Gail-Joon Ann, Bei-Tseng Chu. 2002. 'A Role-Based Delegation Framework for Healthcare Information Systems.' *SACMAT '02 Proceedings of the seventh ACM symposium on Access control models and technologies* 125-134

authorisation can obtain and alter this information provided that their role gives them access. Across organisations, roles for each party should be mapped to each other's equivalent. To share information between different organisations with this technique, actors need to establish mutual trust in the validity of the shared information and roles at the other end of the information exchange. Although it has been a difficult task to build such trust, block-chain mechanisms and shared digital IDs can prove helpful in overcoming the frictions across different governmental organisations.

The second technique is trust-based information sharing.[16] If a centralised trust exists for a third party in the information exchange environment, organisations can share any information they possess with others based solely on their trust for the other organisation. Organisations can manage their trust in other organisations either by ad hoc methods, trust negotiations or credential chain-based trust mechanisms in which multiple trusted third-party actors verify the authenticity of the other organisations before the information is shared.[17]

Introduced by Microsoft in 2016,[18] there is another framework named **A Framework for Cybersecurity Information Sharing and Risk Reduction**, particularly across public and private sector; albeit it can be tailored for specific purposes or sets of actors. It builds the information sharing framework by defining the actors and exchanging information types, models, methods, formats and mechanisms. The model breaks down the types of cybersecurity information into seven items: incidents, threats, vulnerabilities, mitigations, situational awareness, best practices and strategic analysis. The mechanisms of information exchange are split into 'person-to-person' and 'machine-to-machine'. These mechanisms and types of information are classified as formalised, trust-based, security clearance-based and ad hoc. Microsoft's information sharing framework states the principles for incident reporting policies as:[19]

- Aligned to clearly defined outcomes, i.e. protecting privacy, public safety, response coordination, improving defences;
- Flexible policies that leverage commonly accepted approaches and international standards;
- Attentive to balancing the risks and benefits associated with publishing incident details;
- Mapped to specific outcomes, not arbitrary choosing; and
- Supported with research and development in the public and private sectors.

Although not particular to cyber information sharing, the **Government Information Sharing Framework** (GISF) lays out an overarching model that can be tailored to any context, including cyber information sharing across governmental organisations.[20] In its abstract view, the model intersects the concepts (dimensions and maturity stages) of information sharing. The dimensional concepts are environmental, inter-organisational, organisational and technological; and the maturity stages are experience sharing, infrastructure support and information strategy. GISF model offers a robust paradigm, particularly for building an information sharing mechanism from scratch, laying out the focus points in every level. In its detailed composition view, the items are grouped into three stages:

- Stage 1: scope, principle, lifecycle, unit, data component, risk, benefits, barrier;

---

[16] Matt Blaze, Joan Feigenbaum, John Ioannidis, Angelos D. Keromytis. 1996. 'The Role of Trust Management in Distributed Systems Security.' *17th Symposium on Security and Privacy, pages. IEEE Computer Society Press, Los Alamitos* 164-173

[17] Marianne Winslett, Ting Yu, Kent E. Seamons, Adam Hess, Jared Jacobson, Ryan Jarvis, Bryan Smith, Lina Yu. 2002. 'Negotiating Trust on the Web.' *IEEE Internet Computing November - December 02* 30-37

[18] Cristin Goodwin, J. Paul Nicholas. 2015. *A framework for cybersecurity information sharing and risk reduction.* White Paper, Seattle: Microsoft, 2015

[19] Cristin Goodwin, J. Paul Nicholas. 2015. *A framework for cybersecurity information sharing and risk reduction.* White Paper, Seattle: Microsoft, 2015

[20] Estevez, Elsa. 2012. 'Government Information Sharing Network.' Macao: Center for Electronic Governance, United Nations University, 26 November

- Stage 2: best practices, components; and
- Stage 3: initiatives.

Issued for key stakeholders in cyber threat information sharing activities by the National Institute of Standards and Technology (NIST) in the US, the *Guide to Cyber Threat Information Sharing* acts as a detailed and coherent guide for exchanging cyber information between organisations.[21] For information types exchanged between organisations, this model encapsulates the following items:

- Indicators, observables;
- Tactics, techniques and procedures (TTPs);
- Security alerts;
- Threat intelligence reports; and
- Tool configurations.

The biggest benefit offered from the model is that it lists recommendations for each type of cyber threat information and their related sensitive data. Hence, different organisations can adopt and modify the provided recommendations for their unique cases.

Although it is not a complete information sharing system, **Structured Threat Information Expression** (STIX) collection acts as an intermediate language for exchanging and storing cyber threat information. It can be thought of as a superset that also covers other smaller collections like Common Platform Enumeration (CPE), Common Weakness Enumeration (CWE) and Common Attack Pattern Enumeration and Classification (CAPEC).[22] Kornmaier and Jaouen have offered several additions to enhance this collection beyond mere technical cyber information, to increase situational awareness.[23] In this sense, intelligence information from conventional sources was also defined and linked to their correspondent technical ends.

Following the Cybersecurity Information Sharing Act of 2015, the US Department of Homeland Security developed the **Automated Indicator Sharing** (AIS) system.[24] As a free-to-join system by any federal, non-federal or civilian entity, the system's main purpose is to facilitate machine-speed cyber information exchange between its participants covering. Afore mentioned cyber information may include threat indicators, malicious IP addresses, intrusion attempts and phishing emails and so on. AIS operates on STIX[25] and Trusted Automated Exchange of Indicator Information[26] (TAXII) specification for automated data exchange, and guarantees its participants receive broadcast cyber information and have the ability to distribute the received information from the parties. Sharing entities in AIS do not need to disclose their identity as the source of data, hence the information is often anonymous and there is no mechanism of validation embedded in the system, so the emphasis is kept on speed and volume.

---

[21] Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. 2016. 'Guide to Cyber Threat Information Sharing.' *NIST Special Publication 800-150* 3

[22] Barnum, Sean. 2014. 'Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).' *MITRE Corporation*

[23] Andreas Kornmaier, Fabrice Jouën. 2014. 'Beyond technical data - a more comprehensive Situational Awareness fed by available Intelligence Information.' *2014 6th International Conference on Cyber Conflict.* Tallinn: NATO CCD COE Publications. 139 - 154.

[24] US-CERT. 2015. Automated Indicator Sharing. Accessed 02 04, 2019. https://www.us-cert.gov/ais.

[25] *STIX Core Concepts.* 2017 07. Accessed 02 04, 2019. https://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part1-stix-core.pdf.

[26] *TAXII 2.0 Specification.* 19 07 2017.. Accessed 02 19, 2019. https://docs.google.com/document/d/1Jv9ICjUNZrOnwUXtenB1QcnBLO35RnjQcJLsa1mGSkI/pub.

As an inter-state cyber information exchange mechanism, Japan and the US signed an information-sharing agreement in May 2017[27] in which they agreed to share cyber threat indicator information via the AIS system. This agreement and the cooperation appears to be an achievement of the efforts begun with the establishment of the Japan-US Cyber Defence Policy Working Group.[28] The mechanism uses the same principles of AIS in its domestic use, running automated machine-speed data traffic. In this protocol, information sources can stay anonymous if they desire and utilize the internal Traffic Light Protocol (TLP)[29] to provide relevant information packages for its participants.

The **Situational Awareness of Critical Infrastructure and Networks** (SACIN) framework is a proposed development to abstract the complex nature of information received from a wide array of critical infrastructures, and provide a refined common operating picture for decision-makers.[30] It is an agent-based brokered architecture with different nodes running on top of middleware that facilitates centralised event logging and analysis. The proposed framework is promising in that it portrays a logical structure to connect different formats of information generated by different infrastructure systems, mitigating the problem of a common language in cyber information sharing.

Non-standard information exchange protocols, lack of agreed regulations on handling sensitive information and the problems with validating data authenticity eventually have revealed a need for further analysis on aforementioned constraints regarding the cyber defence and security. As a result, **Cyber Security Data Exchange and Collaboration Tool** (CDXI) was designed at the NATO Communications and Information Agency (NCIA) to provide a knowledge management tool for the cyber security domain. It assists information sharing across different bodies, preferably in an automated and refined fashion.[31] CDXI tool sets a number of requirements to overcome the challenges to cyber information sharing. These serve as a starting point for future or ongoing efforts in establishing a more comprehensive framework.[32]

- Providing an adaptable, scalable, secure and decentralised infrastructure based on a freely available core;
- Providing for the controlled evolution of the syntax and semantics of multiple independent data models and their correlation;
- Securely storing both shared and private data;
- Providing for customisable, controlled, multilateral sharing;
- Enabling the exchange of data across non-connecting domains;
- Providing human-machine interfaces;
- Providing collaboration tools that enable burden sharing for the generation, refinement and vetting of data;
- Providing customisable quality-control processes;
- Exposing dissension to reach consensus;

---

[27] Looking Glass Cyber. 2017. *Bridginf the Gap: U.S. & Japan Take an Important Step in Cyber Information Sharing.* 16 11. Accessed 02 04, 2019. https://www.lookingglasscyber.com/blog/threat-intelligence-insights/bridging-gap-u-s-japan-take-important-step-cyber-information-sharing/.

[28] U.S. Department of State. 2017. 'Under Secretary for Public Diplomacy and Public Affairs - Bureau of Public Affairs: Office of Press Relations - Press Releases.' *Joint Statement of the Japan-U.S. Cyber Dialogue.* 24 07. Accessed 02 04, 2019. https://www.state.gov/r/pa/prs/ps/2017/07/272815.htm.

[29] US-CERT. Traffic Light Protocol (TLP) Definitions and Usage. Accessed 02 04, 2019. https://www.us-cert.gov/tlp.

[30] Jussi Timonen, Lauri Lääperi, Lauri Rummukainen, Samir Puuska, Jouko Vankka. 2014. 'Situational awareness and information collection from critical infrastructure.' *6th International Conference on Cyber Confl ict.* Tallinn: NATO CCD COE Publications. 157 - 173.

[31] Luc Dandurand, Oscar Serrano Serrano. 2013. 'Towards improved cyber security information sharing.' *5th International Conference on Cyber Conflict.* Tallinn: NATO CCD COE Publications. 1 - 16.

[32] Dandurand, Luc. 2013. Cyber Security Information Exchange. Accessed 02 04, 2019. https://www.rsaconference.com/writable/presentations/file_upload/sect-t08-cyber-security-information-exchange.pdf.

- Supporting continuous availability of data; and
- Enabling commercial activities.

The CDXI tool, with its proposed requirements and protocols, has been developed as a proof-of-concept form. However, it has not been physically implemented or in use by its targeted stakeholders so far.

4. Challenges to cyber information sharing

Trust issues between different organisations are often responsible for the friction in information flow across both governmental and non-governmental organisations.[33] Trust-based problems refer to an array of reservations of the entities in the cyber information sharing environment. Parties are often if the other party is taking the required precautions to maintain the confidentiality of sensitive information. Even in cases that the parties provide the written internal regulations, which they follow, this usually does not guarantee the desired results. Secondly, keeping sensitive information secure is the owner's responsibility, and if there is a leak from the information shared with third parties, the owners will still be responsible for the failure of keeping sensitive information secure, by law. Third, particularly for the cyber intelligence reports, organisations are not usually eager to share their sources and with other parties. Yet even in the cases where they do not disclose the source, the context of the shared information might reveal the sources' identities.

Authenticating the received information is always a difficult task for organisations and requires dealing with distinct working mechanisms and structures. A significant factor that contributes to the difficulty of sharing information across organisations is that each organisation uses different metrics of assessing the integrity and accuracy of the information. This holds true even when the organisations follow a particular national guide or industry standard.[34] Although they start from the same guidelines of information assessment, human interference and minor modifications for different contexts gradually result in semantic variations.

The other big difficulty of authenticating the accuracy of the information is that the receiving party often has no insight into the previous path the shared information has taken. In many cases, the organisation might want to compare the received information with the corresponding one in their databases (if it exists and is trackable / accessible with low effort) for a weighted sum. However, the received information has the possibility to be modified on its path. Moreover in rare cases, it might even be originated by this same receiver. At this point, keeping track of the nodes the information packages visit seems to be a promising idea, although sharing this kind of metadata might reveal the information sources of the originators. For these reasons, organisations are understandably hesitant to take part in such circulations with applying obligations in place.

Incompatibility of the structures of information between different databases is not specific to cyber information sharing, yet it is still a major challenge. From a structural point of view, every piece of information consists of different parts such as ID code, timestamp, subject, source, expiration date, revision, content and so on. For automated information processing purposes, these information pieces and their respective metadata are often stored in a strict structure. Whereas for ad hoc shared intelligence, the biggest part of the information is usually in plain text format.

Being able to route the cyber information at machine speed and storing the received cyber information in an organisations' own databases with relatively little effort are two of the main benefits to establishing a robust and efficient cyber information sharing mechanism. However, dealing with the multiple inconsistencies among different information formats or even worse, transforming plain text cyber information into a structured format is a tremendously difficult job. Integrating artificial intelligence for parsing human-readable texts into structured format is promising and widely used in certain areas,

---

[33] Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. 2016. 'Guide to Cyber Threat Information Sharing.' *NIST Special Publication 800-150* 4

[34] U.S. Department of Homeland Security. 2017. *National Information Exchange Model.* Accessed 02 01, 2019. https://www.niem.gov/

although in mission-critical systems, the error margin for the task is still high.[35] Given that thousands of information piece would be in circulation in an ideal information sharing framework at machine speed, there is no room for the human-touch for formatting the exchanged information.

Organisations often collect information which is relevant to their operations from open sources, but there may be many reports for each real-life incident in publicly available sources, potentially conflicting with each other. Therefore, when more than one node in an information exchange framework inserts different projections for the same real-life incident into circulation with their respective evaluations, duplicated information increases that could distort the information's authenticity. Unless the context field in these information pieces is used as a key for sorting, which is a complex task that requires human intervention, there appears no practical way to remove recurring duplicate cyber information from information pools.

In the cyber domain, every governmental organisation has its own focused context and area of interest. While a sub-CERT's mission is protecting a nation's finance information infrastructure, the cyber-crime department's concern is mostly concentrated on investigations regarding cyber incidents and forensics. Therefore, using context identifiers before sharing cyber information with other parties in the framework is a useful practice. However, the semantics of each information can differ from the intention of its originator and there is no practical way of assessing the relevancy of given information for another organisation. This complication leads the parties of the information sharing framework to a trade-off between inflating their information database, which brings duplication problems, and failing to possess the data that could prove useful for their area of interest.

[35] Erik Cambria, Bebo White. 2014. 'Jumping NLP curves: A review of natural language processing research.' *EEE Computational intelligence magazine 9.2* 48-57.

5. Best practice

5.1 Acknowledge the actors in the information-sharing environment and define personas

To prevent ambiguities among different organisations that share cyber information and possible intersecting responsibility and authority areas, every organisation and individuals in the system need to be acknowledged and their respective responsibilities and areas need to be designated clearly. The personas do not necessarily point to single individuals or real-time persons; rather they refer to the positions that are filled by the organisation's personnel.

5.2 Setting policies and guidelines for information sharing across governmental and civilian bodies

The most obvious requirement for healthy information sharing across different organisations is having common policies and guidelines guiding the parties on how to conduct their information sharing operations. Albeit in real life, it is arguably the most overlooked aspect in this context.[36] The idea is as simple as having a single and inclusive set of policies and guidelines that regulates cyber information flow across participating organisations, keeping wasted effort at the possible minimum. However, publicly available information sharing strategy documents are generally not designed with future needs in mind. The swiftly evolving cyber context and organisational structures gradually render these policies cumbersome and inefficient. Hence, leaner guidelines and policies that can easily be adapted to evolving needs and structures will prove useful for maintaining cyber information sharing at an optimum level.

5.3 Designating incentives for private organisations to encourage information sharing

In almost all developed countries, core information infrastructure is generally owned and operated by private companies. In an environment where power grids, mobile providers, ISPs, satellite communications and health services reside in the private sector's operational domain, the state's capabilities fall short of its responsibilities regarding the cyber defence of critical information infrastructure. That shortcoming mandates both government and private entities in cyberspace to cooperate and at least maintain a minimum viable information exchange mechanism to sustain their situational awareness.[37]

5.4 Establish an automated framework and formats for rapid information distribution and processing

Mostly applicable to publicly available cyber incidents, related cyber information data travels at machine speed.[38] While the basic structure of data packages is fixed, every organisation can choose different visualisation methods tailored for its own requirements. As one of the core principles of information

---

[36] Pipikaite, Algirde. 2018. *How to stop data leaks.* Periodic Article, World Economic Forum. https://www.weforum.org/agenda/2018/11/how-to-stop-our-leaky-data-connections/

[37] Cristin Goodwin, J. Paul Nicholas. 2015. *A framework for cybersecurity information sharing and risk reduction.* White Paper, Seattle: Microsoft, 15.

[38] Toomey, Fergal. 2015. *Techchrunch - Data, Speed of Light and You.* 08 11. Accessed 02 01, 2019. https://techcrunch.com/2015/11/08/data-the-speed-of-light-and-you/

databases, the information should be as atomic as possible and bigger forms of information can be built by merging multiple atomic data pieces.[39] Although it is not very challenging to circulate cyber information in technical format by using the existing industry standards[40], there is no easy way of breaking down cyber-related intelligence reports into atomic data particles. In this case, adhering to an agreed format across different parties in the information sharing environment gets even more important for organisations in order to share cyber information in complex data packages. Should using this type of mechanism across organisations be achieved, there will be great savings in processing power and human interference requirement for parsing the information.

5.5 Designate rules and official regulations for information sharing

Besides the drawbacks from the government officials' point of view regarding sharing sensitive cyber information and intelligence with other parties, the inability to justify sharing activities in legal terms encourages hesitation. Therefore, setting firm and clear regulations, laws and by-laws regarding the information transactions across governmental organisations is useful in decreasing the risks associated with sharing sensitive information. Enacting positive incentives to attract private parties to get involved in cyber information sharing, as the US recently initiated,[41] will lead to a win-win situation for all involved sides.[42]

5.6 Designate and promote shared goals and benefits for organisations regarding information sharing

It is often easier for different groups to work and cooperate when they share a common goal and this is true of cyber information sharing.[43] The relevance of received information for the organizations' domain increases when information sharing parties have shared goals.

5.7 Set up meetings for overseeing the information sharing process and feedback

Every government organisation across the governments of nations has its unique way of operating and its own distinct internal mechanisms, including in information sharing activities inside these organizations. Like the need for guidelines to effectively conduct cyber information sharing, regular meetings are required to avoid diverting from the mutually assured track of information sharing activities and maintain the shared situational awareness for participating parties.[44,45]

---

[39] Gray, Jim. 1981. 'The Transaction Concept: Virtues and Limitations.' *7th International Conference on Very Large Databases.* Cupertino, CA. 144-154.
[40] FileInfo. 2019. *Database Files.* Accessed 06 11, 2019. https://fileinfo.com/filetypes/database.
[41] U.S. Senate. 2015. 'To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.' *Congress.gov.* 27 10. Accessed 02 01, 2019. https://www.congress.gov/bill/114th-congress/senate-bill/754.
[42] Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. 2016. 'Guide to Cyber Threat Information Sharing.' *NIST Special Publication 800-150* 3.
[43] Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. 2016. 'Guide to Cyber Threat Information Sharing.' *NIST Special Publication 800-150* 3.
[44] Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. 2016. 'Guide to Cyber Threat Information Sharing.' *NIST Special Publication 800-150* 4.
[45] Robert MacFarlane, Mark Leigh. 2014. *Information Management and Shared Situational Awareness: Ideas, Tools and Good Practice in Multi-Agency Crisis and Emergency Management.* Occasional Papers, Series 12, Emergency Planning College.

5.8 Prioritise the information types and areas of importance

In practice, there is an immense amount of cyber information and incident reports travelling between sharing bodies at any given time.[46] Processing and sorting the stream of incoming cyber-related information is a very difficult task, and the task of transferring the information is usually challenging for organisations. To limit the incoming information volume before the processing stage, communicating the prioritised areas of interests to other participants is a very promising practice. By adopting small tailored techniques regarding the shared information prioritisation and preferences, organisations can avoid redundant information traversing back and forth among them and wasting their limited processing power. In best-case scenario, removing unnecessary information from circulation, the number of participants multiplied by the unit of processing power spent per information piece can be saved. Although in practice this is never possible, the benefit well surpasses the effort of establishing the required mechanisms.

5.9 Protection of sensitive and classified information

Civil liberties and privacy of individuals has great importance when it comes to obtaining and sharing cyber information.[47] Improper disclosure of cyber information to partner organisations could result in financial loss, law violations, damage to an organisation's reputation and even legal action.[48] Regulations and by-laws play a crucial role here; hence, following the existing laws regarding information sharing can help participants at being free from possible legal concerns. Periodic and random audits of information confidentiality will help avoid damage and reputation loss.

5.10 Designate integrity and authenticity levels for shared information

As the need of automated information sharing to be consistent in its structure for fast processing mechanisms, having a dedicated data field for the information's integrity and authenticity level can cut out a lot of effort and human interference for classification purposes. The challenge of establishing a fixed evaluation for the integrity of information across different organisations remains,[49] but it is still a big step forward on the path of reducing the resources spent on processing and evaluating received information to insert it into the organisation's own databases.

5.11 Provide feedback mechanisms for received information

Building on the practice of designating integrity and authenticity levels, providing feedback to other parties and committing received feedback into existing information is crucial for maturing the cyber information in the overall information sharing environment. As an incident report, cyber intelligence or other relevant information enters the sharing framework, there is no possibility to check the information's accuracy except indirect methods such as considering the originator's reputation and accuracy level. As parties in the framework enhance the circulating information with their feedback, the quality of the raw data increases in terms of accuracy and authenticity. Feedback can also prove a very powerful tool to rule out stale or inaccurate cyber data and intelligence before it spoils the overall situational awareness picture.

---

[46] Symantec. n.d. *Symantec Security Center.* Accessed 02 01, 2019. https://www.symantec.com/security-center
[47] European Union. 2016. 'Official Journal of the European Union L 119.' *EUR-Lex.* 04 05. Accessed 02 01, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC.
[48] Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. 2016. 'Guide to Cyber Threat Information Sharing.' *NIST Special Publication 800-150* v.
[49] Peng Liu, Amit Chetal. 2005. 'Trust-based Secure Information Sharing between Federal Government Agencies.' Journal of the Association for Information Science and Technology.

6. Conclusion

Governmental organisations usually have limited budgets and wide areas of responsibility, hence any improvement in terms of cutting costs or increasing effect is to their benefit. In today's vast cyberspace arena, it is practically impossible for a single organisation to track and process all the information and use it for its operations. Hence establishing and maintaining a robust, fast-acting information sharing mechanism across governmental organisations promises the desired effectivity increase. It is clear that there are some natural challenges to this, but following and internalising good practices by all actors in the framework will assist the organisations to operate more efficiently. Moreover, it will also likely carry them to a better point of view, from which different prospective solutions to challenges may appear.

The measures of success on the path to more efficient information sharing across governmental organisations can be grouped in five areas. The information sharing practice between the organisations, independent from its means and models, should be fast, preferably at machine speed, and the received information should be as accurate as possible while remaining relevant to the area of operation. Parties to the information sharing framework need to assure each other about the confidentiality practices for shared data. Finally, the information in circulation should always be complete while staying as atomic as possible for structural concerns.

Nations with robust, concurrent and fast information sharing mechanisms across their governmental organisations will reduce wasted resource and human effort spent on recurring tasks by different parties. The information that was not available is also processed and fed to them almost at the final maturity level, without spending much human labour or processing power. As the conclusion, all organisations involved in the information sharing framework can experience a dramatic increase in situational awareness while staying inside their desired budget.

References

Agrawal Rakesh, Alexander Evfimievski , Ramakrishnan Srikant. 2003. “Information sharing across private databases.” *SIGMOD '03 Proceedings of the 2003 ACM SIGMOD international Conference on Management of Data* 86-97.

Andreas Kornmaier, Fabrice Jouën. 2014. “Beyond technical data - a more comprehensive Situational Awareness fed by available Intelligence Information.” *2014 6th International Conference on Cyber Conflict.* Tallinn: NATO CCD COE Publications. 139 - 154.

Barnum, Sean. 2014. “Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).” *MITRE Corporation.*

Centre for Strategic & International Studies. 2019. *Significant Cyber Incidents.* January. Accessed January 30, 2019. https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, Clem Skorupka. 2016. “Guide to Cyber Threat Information Sharing.” *NIST Special Publication 800-150.*

CNBC. 2017. *There are 20 billion cyber attacks every day: Cisco.* 11 May. https://www.cnbc.com/video/2017/05/11/there-are-20-billion-cyber-attacks-every-day-cisco-.html.

Cristin Goodwin, J. Paul Nicholas. 2015. *A framework for cybersecurity information sharing and risk reduction.* White Paper, Seattle: Microsoft, 15.

Dandurand, Luc. 2013. *Cyber Security Information Exchange.* Accessed 02 04, 2019. https://www.rsaconference.com/writable/presentations/file_upload/sect-t08-cyber-security-information-exchange.pdf.

Erik Cambria, Bebo White. 2014. “Jumping NLP curves: A review of natural language processing research.” *EEE Computational intelligence magazine 9.2* 48-57.

Estevez, Elsa. 2012. “Government Information Sharing Network.” Macao: Center for Electronic Governance, United Nations University, 26 November.

European Union. 2016. “Official Journal of the European Union L 119.” *EUR-Lex.* 04 05. Accessed 02 01, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC.

FileInfo. 2019. *Database Files.* Accessed 06 11, 2019. https://fileinfo.com/filetypes/database.

Goldreich, Oded. 2002. “Secure Multi-Party Computation - Draft Version 1.4.” *Department of Computer Science and Applied Mathematics, Weizmann Institute of Science.*

Gray, Jim. 1981. “The Transaction Concept: Virtues and Limitations.” *7th International Conference on Very Large Databases.* Cupertino, CA. 144-154.

ICS-CERT. 2012. *Joint Security Awareness Report (JSAR-12-241-01B) Shamoon/DistTrack Malware (Update B).* 16 October. https://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B.

Jussi Timonen, Lauri Lääperi, Lauri Rummukainen, Samir Puuska, Jouko Vankka. 2014. “Situational awareness and information collection from critical infrastructure.” *6th International Conference on Cyber Confl ict.* Tallinn: NATO CCD COE Publications. 157 - 173.

Longhua Zhang, Gail-Joon Ann, Bei-Tseng Chu. 2002. “A Role-Based Delegation Framework for Healthcare Information Systems.” *SACMAT '02 Proceedings of the seventh ACM symposium on Access control models and technologies* 125-134.

Looking Glass Cyber. 2017. *Bridginf the Gap: U.S. & Japan Take an Important Step in Cyber Information Sharing.* 16 11. Accessed 02 04, 2019. https://www.lookingglasscyber.com/blog/threat-intelligence-insights/bridging-gap-u-s-japan-take-important-step-cyber-information-sharing/.

Luc Dandurand, Oscar Serrano Serrano. 2013. “Towards improved cyber security information sharing.” *5th International Conference on Cyber Conflict.* Tallinn: NATO CCD COE Publications. 1 - 16.

Marianne Winslett, Ting Yu, Kent E. Seamons, Adam Hess, Jared Jacobson, Ryan Jarvis, Bryan Smith, Lina Yu. 2002. “Negotiating Trust on the Web.” *IEEE Internet Computing November - December 02* 30-37.

Matt Blaze, Joan Feigenbaum, John Ioannidis, Angelos D. Keromytis. 1996. “The Role of Trust Management in Distributed Systems Security.” *17th Symposium on Security and Privacy, pages. IEEE Computer Society Press, Los Alamitos* 164-173.

Moni Naor, Kobbi Nissim. 2001. “Communication Preserving Protocols for Secure Function Evaluation.” *STOC '01 Proceedings of the thirty-third annual ACM symposium on Theory of computing* 590-598.

Morgan, Steve. 2017. *Cybersecurity market slowdown? Not anytime soon.* Business Report, CSOOnline. https://www.csoonline.com/article/3242811/security/cybersecurity-market-slowdown-not-anytime-soon.html.

Online Trust Alliance. 2018. *Cyber Incident & Breach Trends Report.* Annual Report, The Internet Society. https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf.

Peng Liu, Amit Chetal. 2005. “Trust-based Secure Information Sharing Between Federal Government Agencies.” *Journal of the Association for Information Science and Technology.*

Pipikaite, Algirde. 2018. *How to stop data leaks.* 07 11. Accessed 02 01, 2019. https://www.weforum.org/agenda/2018/11/how-to-stop-our-leaky-data-connections/.

Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman. 1996. “Role-Based Access Control Models.” *IEEE Computer, Volume 29, Number 2* 38-47.

Robert MacFarlane, Mark Leigh. 2014. *Information Management and Shared Situational Awareness: Ideas, Tools and Good Practice in Multi-Agency Crisis and Emergency Management.* Occasional Papers, Series 12, Emergency Planning College.

Stevens, John. 2018. *Internet Stats & Facts for 2019.* 17 December. Accessed 01 30, 2019. https://hostingfacts.com/internet-facts-stats/.

2019. *STIX Core Concepts.* 2017 07. Accessed 02 04, 2019. https://docs.oasis-open.org/cti/stix/v2.0/stix-v2.0-part1-stix-core.pdf.

Symantec. n.d. *Symantec Security Center.* Accessed 02 01, 2019. https://www.symantec.com/security-center.

2017. *TAXII 2.0 Specification.* 19 07. Accessed 02 19, 2019. https://docs.google.com/document/d/1Jv9ICjUNZrOnwUXtenB1QcnBLO35RnjQcJLsa1mGSkI/pub.

The Wall Street Journal. 2017. *The Fight Against Nation-State Cyberthreats.* 18 December. Accessed January 30, 2019. https://www.wsj.com/articles/the-fight-against-nation-state-cyberthreats-1513653060.

The White House. 2012. *National Strategy for Information Sharing and Safeguarding.* Official Strategy Document, Washington: The White House.

Toomey, Fergal. 2015. *Techchrunch - Data, Speed of Light and You.* 08 11. Accessed 02 01, 2019. https://techcrunch.com/2015/11/08/data-the-speed-of-light-and-you/.

U.S. Department of Homeland Security. 2017. *National Information Exchange Model.* Accessed 02 01, 2019. https://www.niem.gov/.

U.S. Department of State. 2017. “Under Secretary for Public Diplomacy and Public Affairs - Bureau of Public Affairs: Office of Press Relations - Press Releases.” *Joint Statement of the Japan-U.S. Cyber Dialogue.* 24 07. Accessed 02 04, 2019. https://www.state.gov/r/pa/prs/ps/2017/07/272815.htm.

U.S. Senate. 2015. “To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.” *Congress.gov.* 27 10. Accessed 02 01, 2019. https://www.congress.gov/bill/114th-congress/senate-bill/754.

US-CERT. 2015. *Automated Indicator Sharing.* Accessed 02 04, 2019. https://www.us-cert.gov/ais.

—. n.d. *Traffic Light Protocol (TLP) Definitions and Usage.* Accessed 02 04, 2019. https://www.us-cert.gov/tlp.