AARMS Vol. 17, No. 3 (2018) 131–148. 10.32565/aarms.2018.3.9

Interoperability Services Supporting Information Exchange Between Cybersecurity Organisations[1]

Sándor MUNK[2]

The security of cyberspace can be ensured by a broad cooperation of different organizations, actors. This cooperation cannot be achieved without interoperable information exchange between cybersecurity actors, organisations, and their IT systems. Interoperable information exchange can be realized using own resources, or using services provided by third parties. IT interoperability service can be defined as a service by which a service provider supports interoperable data exchange between IT systems of service consumers and cooperating actors. This publication provides different categorizations of interoperability services, discusses their benefits, and the necessary user tasks. It determines the types of interoperability service providers and their necessary capabilities. Finally, it defines the special requirements of cybersecurity information exchange and presents the main types of required services.

Keywords: *interoperability, cybersecurity organisations, interoperable information exchange, IT services*

Introduction

Today's social, economic and everyday activities are increasingly dependent on the services provided by globally interconnected, decentralized IT systems and networks that make up the cyberspace. This dependency also means increasing vulnerability and risks. A secure cyberspace, cybersecurity requires a broad range of actors and extensive cooperation, collaboration. It is also clear that successful and effective cooperation is not possible without a similar level of information exchange.

Information exchange between different actors may have and in practice almost always has interoperability problems that require appropriate solutions. This is also the case for the various actors of cybersecurity scene, which include event management centres, operations centres, organisations providing cybersecurity information and IT developers, manufacturers.

Solutions for ensuring and maintaining interoperable exchange of information between IT systems of the actors involved can be implemented by the actors themselves, or they can use services provided by third parties. With the emergence and spread of cloud-based technology, the role of services is gradually increasing. This makes it necessary to examine

[1] The work was created in commission of the National University of Public Service under the priority project PACSDOP-2.1.2-CCHOP-15-2016-00001 entitled "Public Service Development Establishing Good Governance" in the Ludovika Cybersecurity Workshop.

[2] DSc, Professor, National University of Public Service, Faculty of Military Sciences and Officer Training, Institute of Military Maintenance; e-mail: munk.sandor@uni-nke.hu

the possibilities of services supporting interoperable information exchange in general, and in particular for cybersecurity information exchange.

The purpose of this research paper is to outline the basics and the framework of using IT interoperability services to ensure and maintain interoperability during exchange of information between cybersecurity organisations. For this reason it:

- discusses the concept and elaborates the definition of IT interoperability services supporting information exchange;
- suggests classification criteria and classifies IT interoperability services supporting information exchange;
- determines the benefits of using such services and the tasks to be performed;
- determines the types of service providers of such services and their necessary capabilities;
- summarizes the interoperability problems and solutions of the exchange of cybersecurity information;
- identifies possible types and content of cybersecurity interoperability services.

Basics of Interoperability Services

To examine the interoperability services that support the exchange of information between cybersecurity organizations, we first need to summarize the basics of interoperability services. In today's literature, though we may encounter the term, there is no mature definition, or practically, there is not even a definition of the concept of interoperability services. For this reason, I will start from the components of the term, so I will simply consider it a service that supports interoperability.

Interoperability itself is a widely used concept that is in many respects clearly defined, but it has a number of types modified by an adjective. In the following, I will briefly summarize the basics of information interoperability and IT interoperability, their concepts, problems, levels and solutions, largely based on my previous publications. [1] [2] [3]

I will then elaborate the definition of the information interoperability service and then the definition of IT interoperability service concepts used in this publication, and then present the most important occurrences of these terms in the literature. Next, I sum up and analyse the technical implementation forms of interoperability services. Finally, I give a more precise definition of the interoperability service.

Basics of Information Interoperability

A fundamental prerequisite of cooperation between cybersecurity organizations is the effective and efficient exchange of information that meets the information needs of the parties and which can be used in their activity. Its conditions are ensured by the interoperability between organizations and their IT systems.

Information interoperability is a type of the general concept of interoperability, related to the exchange of information between the cooperating actors. Under the concept of interoperability, in general terms, we mean a mutual capability between/among two or more objects, necessary to ensure successful and efficient interoperation, supporting cooperation. Accordingly, information interoperability is the mutual capability of different actors (persons, organizations, groups) necessary to ensure exchange and common understanding of information needed for their successful cooperation. In case of information interoperability, information is transmitted between the actors in a meaning-preserving mode, at a necessary level for their cooperation. Since all cooperation is based on the exchange of information between participants, information interoperability is a necessary condition for any "higher level" (e.g. organizational) interoperability.

Exchange of information between actors can take place directly between people, between people and their IT systems, as well as between IT systems. In case of traditional exchange of information between people, the preservation of meaning is based on the existing knowledge, experience of previous cooperation and cognitive abilities of the peoples. Nowadays, however, there is an increasing importance of the exchange of information between the actors' IT systems without human interaction, which requires the introduction of another concept.

The *IT interoperability* is a mutual capability of IT systems, devices and applications to receive, provide, i.e. exchange data—using transformations if necessary—preserving the meaning assigned to data by their primary users to the extent necessary for their cooperation. The data itself does not have any meaning, it is essentially a fixed representation of information, to which only their producers and their users assign (intended or interpreted) meaning.

An ***information interoperability problem*** arises only if there are some differences between the cooperating parties, when heterogeneity is present. In terms of information interoperability, heterogeneity and thus interoperability problems can be divided into levels to which independent interoperability types and capabilities belong. The difficulties in the meaning-preserving information exchange by the consensus of the literature can be grouped into three levels, which are:

- the technical level of physical media used in the exchange of information;
- the syntactic level of the language, message and data formats used;
- finally, the semantic level of the content and meaning to be transmitted.

Technical level information interoperability is a set of capabilities to handle, produce, transmit, display material (physical) representations by "interoperable" devices. Nowadays, IT technology ensures the storage and exchange of practically arbitrary representations based on continuous bit streams and finite bit sequences.

Syntactic level information interoperability is a set of capabilities to manage—produce, process and present—intermediate representations in the form of data, based on material representations. These include numerical representations, string formats, character code tables, data structure representations, digital representations of textual and drawing information, and digitized formats of sampled audio, visual and other sensory information. Although the scope of possible syntactic representations is wide, in practice they are limited to a relatively small number of standard solutions.

Semantic level information interoperability is a set of capabilities that make use of the intended meaning of syntactic level representations that carry information. In case of IT systems, the proper interpretation of the received data requires additional knowledge about the meaning of that type of data. Previously, this knowledge was embedded, "hidden" in algorithms (programs). Nowadays, the amount of semantic information manageable by IT tools about the connection between data and their meaning has been significantly expanded. This includes data about data (metadata) as well as formalized concept systems (controlled dictionaries, taxonomies, ontologies).

Elimination of interoperability problems, maintaining the necessary interoperability can be achieved by ***interoperability solutions.*** One of the interoperability solutions is standardization, reduction or elimination of heterogeneity; the other is the insertion of meaning-preserving transformations between the form used by the sending (data providing) party to the form used by the receiving (data receiving) party.

The *technical and syntactic level interoperability solutions* must ensure that the different material (physical) resources and target representations involved in the transformation carry the same syntactic representation (digital bit sequence, bit stream), and that the different data formats and structures of source and target sides be transformed to each other preserving the meaning to the necessary extent. While technical level solutions in principle can transform bit sequences and streams without loss of information, it is not true for syntactic level transformations. Some syntactic representations cannot be transformed unambiguously to each other.

The most difficult task is to develop *semantic level solutions*. The details of solutions on technical and syntactic levels are of no interest for the users, and can be replaced invisibly, not affecting their activity. By contrast, the meaning assigned to the data processed, the concepts used in the interpretation, and their relationships are closely related to the user activity. Thus, standardization is not always a solution, heterogeneity cannot be completely eliminated or it is not straightforward to eliminate.

Nowadays, practically all IT interoperability solutions are based on the use of agreed (standard) intermediary representations. In this case each actor stores the information in the form of his/her own internal representation and after transformations, it is transmitted in the form of the intermediary representation. This solution leaves the autonomy of the individual actors, does not deal with the internal representations they use, with the possible syntactic and semantic differences (possibly) existing between them and with the tasks of transformation between the internal representation and the intermediary representation. It allows new entrants to flexibly engage in the interoperable exchange of information within the scope of cooperation, without the original actors having new transformation tasks.

Concept and Interpretation of Interoperability Services

There are several possibilities for implementing information (and IT) interoperability, requiring tasks with different content and difficulty. In case of all tasks, such as the creation of the conditions for interoperability, there are two possibilities: a solution based on own resources or provided by an external service provider. In the following, I will examine the concept of information and IT interoperability service and their different interpretations.

In general terms, the ***service*** is an activity that is intangible, a service provider provides to its customers which is of value to the recipients. The use of a service may be justified by the fact that the activity provided:

- cannot be performed by the consumer in the absence of resources or capabilities;
- or the activity's own implementation is less efficient and economical.

Different types of services are distinguished: what benefits they offer to their customers (what results they bring, what their activities support and what activities they perform in place of them).

Information interoperability service is, accordingly, a service by which the service provider supports the interoperable exchange of information between the service consumer and other parties. The interoperability service may provide interoperability conditions in whole or in part. In case of traditional information exchange, an old "interoperability service" is interpreting.

Similarly, the concept of ***IT interoperability service,*** which is relevant to our subject, can be defined as a service by which the service provider supports interoperable (meaning-preserving) data exchange between the information system, tool and application of the service consumer, and the IT systems, tools and applications of other actors. The basic task of an IT interoperability service (hereafter shortly referred to as interoperability service) is the transformation between the internal representation of the information handled by the given actor and the intermediary representation, so the essence of interoperability services is the support and implementation of such transformations.

The meaning-preserving transformation of data was already mentioned in the early 1990s in the form of *mediation services,* in relation to IT systems processing data from heterogeneous sources.

Mediators provide intermediary services, linking data sources and applications, so they do not have to deal with uninteresting differences and details of their solution. Mediators provide integrated information without the need for integration of data sources. [4] Data mediation is a semantic transformation of data structures and data content that maintains semantic equivalence between different representations. [5]

The term ***interoperability service in the literature*** is described in several different forms, mostly without precise definition, most of which denote a component of a software architecture, a software service type that is a functionality provided by a software component to another software component through a defined interface.

The *Interoperability Service Utility* is one of the basic concepts of the *Cooperation and Interoperability for Networked Enterprises* (COIN) project 2008–2011 of the European Union's 7th Framework Program for Research, which is a utility-like capability, provided as a service, that establishes organizational interoperability. [6] The term has already been used in the roadmap of enterprise interoperability research project, as a layer of the open cyberspace, sitting atop of the Internet, and the Web. [7: 2]

The term appears in the title of the Content Management Interoperability Services (CMIS) standard of Organization for the Advancement of Structured Information Standards (OASIS) published in 2010 and modified in 2015. The purpose of the standard is to support information sharing between content management repositories/systems made available by different service providers, by specifying web services and interfaces. [8]

Message-oriented middleware services and *mediation services* are included in the list of services of NATO C3 Classification Taxonomy, released in 2012 and further developed in 2015, in the group of service-oriented architecture platform services of the core technical services. The platform services provide a foundation to implement web-based services in a loosely coupled environment, ensuring flexible, adaptable alignment and coordination of services, and can be used as a capability integration platform in a heterogeneous service-provisioning ecosystem. [9: 33–34]

Technical implementation forms of interoperability services include middleware services, web services, and cloud-based services. In the literature one can find published concepts and expressions related to interoperability services, and connected to these implementation forms.

Middleware is a software product that provides its own value-added services to applications. Middleware services can complement the operating system features, support collaboration of shared software components, or provide access to various objects (e.g. data, documents, databases). Our topic is best served by the following definition: "Middleware is the software that assists an application to interact or communicate with other applications, networks, hardware, and/or operating systems." [10: 254] As it can be seen from the definition, the main but not the only function of the middleware is to ensure interoperability. In this context we can find the term "middleware services for interoperability" in the literature.

Web services in general are software services provided through the World Wide Web, between software components, in practice, in the strict sense, services that meet the W3C Web Services standard package. According to the latter, the web service is a software system designed to support interoperable machine-to-machine interaction over a network, according to certain web standards.[3] [11: 1.4] Web services are a concrete implementation of the service-oriented architecture (SOA). In this context, the term mediation web services also appear in the literature.

Cloud services are IT services that can be accessed and activated on demand via Internet from a cloud computing provider, and their costs are generally proportionate to usage. Services are built, operated and managed by the cloud service provider. In addition to conventional cloud services,[4] the concepts of "interoperability as a service" and related to this "interoperability service provider" have appeared.

Hereinafter, the interoperability service is considered only a solution in which the functionality of interoperability between IT systems, devices and applications is realized, and is provided by an interoperability service provider, independent of the consumer. Of the three technical implementation types described above, only interoperability cloud services and interoperability web services (or service-oriented architecture services) are operated by independent service providers. We do not include interoperability middleware solutions because, in these cases, the operator of the "service provider" software component is also the same as of the application using the service.

Types of Interoperability Services, their Role in the Implementation of Interoperability

Implementing functions as a service that support the interoperability of IT information systems, tools, applications and meaning-preserving exchange of information, as well as

[3] It has an interface described in Web Services Description Language (WSDL) format, interaction is done by Simple Object Access Protocol (SOAP) messages (typically conveyed using HTTP with an XML serialization).

[4] Infrastructure as a Service, Platform as a Service and Software as a Service.

the range of such services is still limited. In different application areas the basic solution for ensuring and maintaining interoperability of IT systems is the use of agreed, standardized intermediary representations. Implementing a solution based on this is a complicated task, and the cooperating systems have to carry out a significant part of that.

In order to ensure IT interoperability, the systems involved in the cooperation will implement a number of functions that could be utilized or have already been implemented in other systems. Instead of developing, maintaining or improving these features and capabilities, they can be used more efficiently and more economically as services.

In the following, to analyse the aspects of the use of interoperability functions as a service, I will present the main classification criteria, types and characteristics of these services, then examine the benefits and tasks of the services from the user point of view, as well as the types of service providers and their necessary capabilities.

Types of Interoperability Services

Interoperability services can be categorized according to different criteria. In the following, I briefly present some of the classification criteria considered relevant, the related types and their main features.

Interoperability services, according to their level may be syntactic and semantic. Among these I do not count physical level interoperability services, because these are tasks of the communication infrastructure, and today these functions are essentially ensured by IP-based data exchange available on all transmission technology.

Syntactic level interoperability services provide meaning-preserving transformations between data element representations and data structures built up from data elements. The first group includes transformations between elementary data representations corresponding different specifications. During the transformation, the content of the information carried by the data element may not be completely preserved because of the difference between source and target value sets.[5] The syntactic level data element transformations are independent of the application area, knowing the rules of the two representations they can be implemented without any application domain knowledge.

The second group is the transformations between data structure representations. These include transformations between different representations of elementary data structures and transformations between different document formats.[6] Data structure transformation interoperability services transform a source data structure representation into a target data-structure representation, provided that all data elements of the target can be generated from the data elements of the source. These services, therefore, utilize the services provided by the syntactic data element transformations.

From the point of view of syntactic data structure transformations, general purpose markup languages for semi-structured data as well as standard message formats are of paramount importance. Among the former, today the XML format is dominant, but JSON format is

[5] For example, lower numerical accuracy, smaller character count, narrower character set, or lower image colour depth.

[6] For example text, drawing, audio, video, or complex document formats.

also worth mentioning that are application area independent.[7] Standard message formats are predominantly based on these two formats and textual formats that meet simple rules.

Semantic level interoperability services provide transformations at the level of meaning of the information carried by data (independent of representation format). Both data elements and data structures contribute to the meaning, so accordingly the semantic transformations can also be split into two groups.

Among the elementary semantic meaning-preserving transformations, the conversions between different units of measurement, dates given in different calendar systems, or classifications belonging to different classification systems play a significant role. In general terms, the transformation of textual descriptions between different languages or translations of texts into foreign languages should also be considered as a semantic transformation.

As stated earlier, the data alone do not have a meaning, so the meaning-preserving transformation requires additional knowledge that can be "wired" into the transformation software component or be available in the form of semantic information related to the meaning of data. Semantic level interoperable transformations—as opposed to syntactic level transformations—can only be achieved by using specialized application domain knowledge. The rules of the transformations, the order of their implementation, or the semantic information required for this purpose must be determined by domain area specialists. If a transformation that not always, or not completely preserves meaning is acceptable, and the conditions are available, semantic level transformation can be achieved by artificial intelligence solutions based on machine learning.

Interoperability services, according to their nature can be classified into two broad categories. The first includes *services implementing transformation subfunctions,* that are used by one party involved in the exchange of information to transform one part of the information to be transmitted. In this case the parts of the transformation, not supported by services, from the own internal representation to the intermediary representation, or in the opposite direction, and the sending or receiving of the intermediary representation are the responsibility of the party concerned.

The second group is the *services implementing a complete meaning-preserving information exchange.* In this case, the service takes over the information to be transmitted from the sender, transforms it to the extent necessary and transmits it to the receiver(s). This solution is also referred to as an interoperability gateway for the analogy of the tools used for physical level information exchange, and which can also be provided as a service.[8]

An essential characteristic of interoperability services providing complete information exchange is the representations and protocols they "know", among which they provide meaning-preserving transformations. Among them, like in case of other types of gateways, it is expected that standardized representations will be used. Thus, the transformation between the individual internal representations of the actors and the standard intermediary representations remains the responsibility of the actors. The main purpose of the gateways is to interconnect different cooperation groups and the transformation between their intermediary representations.

[7] Extended Markup Language, JavaScript Object Notation.

[8] See for example the NATO Information Exchange Gateway, [12] the Medical Interoperability Gateway of the Healthcare Gateway company, [13] or the Semantic Gateway as a Service solution of the Internet of Things paradigm. [14]

Interoperability services, according to their availability may be publicly available to anyone, or closed, accessible only to the members of a cooperation group. *Public interoperability services* include, for example, freely available document format conversion services (voice, video, text, document, presentation, e-book, archive, etc.) on the Internet. Most of these are accessible via a manual user interface, but many service providers also provide programmed access, in the form of web services.[9] These may be free or pay-per-use cloud-based services. In case of public services, safety considerations must also be taken into account as the information to be transformed becomes accessible to the service provider.

Closed interoperability services are a safer solution provided by internal providers under the control of a particular user group, or by trusted external service providers. The availability of services can be restricted to closed networks or controlled by access rights. Closed interoperability services may be needed, inter alia, for public administration, the defence sector and the cooperative IT systems of the European Union or NATO. In case of European and national public services, closed service can be provided by the previously mentioned interoperability service public utility.

Users of Interoperability Services

Users of interoperability services are cooperating actors, who exchange information with each other and wish to create the conditions of the meaning-preserving information exchange using the services provided by service providers.

The ***benefits of interoperability services for users*** are essentially the same as the benefits of services in general. Services provide capabilities, perform activities that their users cannot, or they would only at an expense, compared to which the service is more economical.

The basic type of interoperability services is a meaning-preserving transformation between information representations (data), ranging from transforming certain data elements, to transforming messages, and connecting information exchange protocols. This is accomplished through software components that can also be obtained as a product, so the question arises why software components that can be embedded in your system are not worthy of use as services.

The traditional reasons for the use of services in general are also true for interoperability services: their total costs are lower, they can be used timely, without preparatory tasks, the service levels can be guaranteed, operational and maintenance tasks are not the users responsibility. Because of the information exchange standards change from time to time, newer versions will be introduced, special expertise, software modification and development will be required to track these, but this is the responsibility of service providers rather than users.

In case of interoperability services, there are also ***user tasks.*** As interoperability services are expected to relate to more widely used, standardized representations, they support the use of meaning-preserving transformations between such representations, specific transformations need to be implemented by users between user specific internal representations and

[9] For example, ZamZar Online file conversion, online-convert.com, ConvertAPI.

representations known by interoperability services. Let us examine where they are needed, and where they are not and where services are probable.

The number of different representations of the *first group of general data elements* (such as numbers, logical values, dates, times) is relatively low, less dependent on the application area, the transformations that can be made between them are well formalized and can be easily implemented so that they can be provided as adequate interoperability services.

Different representations of *another group of general data elements* (character strings, unformatted texts: names, short descriptions, remarks etc.) can differ in two ways: the character set used and the language. The range of the former is also limited, so transformation services between them exist, and will exist in the future. Furthermore, to resolve language differences, there already exist— in fact not yet perfect—services in the form of machine translation capabilities.

Finally, interoperability services already exist in the form of easy-to-use conversions between different formats of *audio, video and video information.*

In case of *classification data elements (categories or types),* interoperability services between the different versions of these are required only for widely used standard versions. To develop such a transformation, and a service implementing it are made more difficult by the fact that there is usually no unambiguous mapping between the different classification systems, working in both directions. Nonetheless, when exchanging such information, accepting some loss of information, through the use of an “other, cannot be classified” category, the transformation could be done with preserving the most possible information.

The meaning-preserving transformation between *different formats of data sets* (messages, composite documents) is a complex task, including the necessary transformation of data elements that constitutes the data-set, as well as their relationship structure, the data describing this structure. The questions related to data elements we have been discussing above and in case of data structures, based on the fact that a significant part of these structure formats[10] is of general purpose, standardized, widely used, and interoperability services are already expected to appear.

Providers of Interoperability Services

Interoperability services cannot exist without service providers, so there should be actors that create these services, maintain the conditions for their provision and make it available to the consumers who use the service. The benefits of implementing interoperability functions in the form of a service include the concentration of the capabilities required for the functions, the wider availability of functions and therefore the more economical operation and the more efficient maintenance of functions.

Interoperability providers according to their type may be third party market-based providers working independently of the consumers of their services, or may be internal service providers supervised by some user community. *Third-party service providers* may offer interoperability services in the public domain, mainly on syntactic and elementary

[10] Nowadays, these formats are primarily at the elementary level, the XML; at the upper levels are the different message format or document format standards.

semantic level, but may also operate interoperability gateways if there are user needs. In case of the former, service providers use these services to promote their other similar products, while in case of the latter it is more likely to sell interoperability gateways as products, complemented by a service package that includes further development.[11] In my view, in case of organizational actors, the use of external service providers will be limited due to security, reliability and availability considerations.

Internal service providers typically provide closed services (available to a particular user community), and their services, less frequently, could be open. They serve organizational purposes, the information exchange within a stable cooperating community, the integration of heterogeneous IT systems. The implementation of functions supporting the meaning-preserving information exchange as a service enables the functional separation of the functions and tasks of the organizations involved in the operation of IT systems and of the organizations, organizational elements providing interoperability services.

The ***capabilities necessary for interoperability services*** in case of syntactic level services are easier to develop and do not require deep application area expertise. Conversely, much of the information needed for the transformation at the semantic level is not readily produced. Among them, the transformations between different classifications are a top priority.

The *reasons for different classifications* lie in the different needs and perspectives of their users. Different application communities can group the same objects into different classes, according to their own interests, to their own criteria. There may be a difference between the range of objects to be categorized, and a user community can also create classes for objects that are not in the interest of other communities. Differences between classifications cannot usually be eliminated, in the vast majority of cases there is no way to create and apply a single classification system that is equally suitable for all users.

The *transformation between the different classification systems* means practically a conversion between classification characteristics: based on the source side classification value the target side classification value should be determined. The result of the conversion may be that for the source classification does not exist an appropriate classification value on the target side (or, if there is, it is only the "other"). Therefore, conversion requires further knowledge, for example other attributes describing the source object. Depending on the nature of the relationships and differences between the two classification systems, from the point of view of the source, a transformation may be a one-to-one mapping, it may require additional information (knowledge of other characteristics) and may not be feasible. Conversion between two classification systems, in many cases, is not symmetrical: it can be performed in one direction (e.g. from a more detailed classification into a more comprehensive classification) and in the other it cannot, or only partially.

Service providers that provide transformations between classification systems may be the organizations responsible for the definition of classification systems, or may be independent service providers. The former, of course, has better capabilities and opportunities to determine the content of the meaning-preserving transformation. In case of modification of the classification system on the same application domain, the responsible organization is

[11] For example, in the military application, the IRIS MTF Gateway and IRIS Information Mapping of the Systematic company, as well as the Oracle EDI Gateway products in civil application.

able and is entitled to define the rules of the conversion.[12] In case of a transformation between a classification system supervised by two different organizations, the definition of rules may be the result of joint work, or may be done by one party that is more interested in ensuring the possibility of conversion from another classification system to its classification system.

Interoperability Services in Cybersecurity Information Exchange

Today's social, economic, and everyday activities are increasingly dependent on the services provided by the interconnected, decentralized IT systems and networks that make up the cyberspace. Increasing dependence also means a growing vulnerability and risk, as the breach of the security of IT systems, networks and of information and data that they manage will also result in harm to security of these services. Every state, and every organization must be ready to manage the risks and handle the threats in cyberspace to ensure an adequate level of cyber security. The creation and maintenance of cybersecurity requires a wide cooperation involving several actors, based on the exchange of cybersecurity information.

The cybersecurity information exchange, like other areas of expertise, is hampered by differences and heterogeneity between the actors involved and the IT systems they use, due to their different purposes, approaches and solutions, which require an interoperability solution. One of the possibilities of creating and maintaining interoperability between the actors' IT systems is the implementation of interoperability functions in the form of services.

In the following I will first summarize the basics of cybersecurity information exchange and its interoperability problems and solutions; next, I identify the possible types and content of the syntactic level and then the semantic level of cybersecurity interoperability services.

Cybersecurity Information Exchange, Interoperability Problems

For the purpose of exploring and analysing interoperability services supporting cybersecurity organizations in the following, based on two of my previous publications, I first summarize the framework for cybersecurity information exchange, [15] then the interoperability problems and solutions for information exchange. [16]

Cybersecurity information is all the information that actors involved in cybersecurity[13] are using to perform their tasks. This information can be divided into four major groups (information related to events, to vulnerabilities, to threats, and other information).

Information related to cybersecurity events consists of primary raw event information and evaluated event information. These include the information about the person, organization reporting, the dates and the description of the event; its classification; the components involved, the consequences and effects of the event; and its roots, causes and course. Cybersecurity organizations are continuously receiving, analysing, and, where necessary,

[12] For example the Hungarian Statistical Classification of Economic Activities (TEÁOR).

[13] Cybersecurity emergency response organizations, cybersecurity operations centres, other cybersecurity organizations (providing information, detecting and analysing threats) and vendors of IT products.

transmitting information about the events to the organizations under their responsibility (constituents), and to the cooperating organizations.

Cybersecurity actors maintain and use global and organizational level databases about *cybersecurity vulnerabilities* for their activities. These databases contain the identification and description of vulnerabilities; the components involved, the consequences, and the assessment and severity of the exploitation; the possible ways and methods of exploitation, and its tools already known; as well as the solutions that eliminate, or minimize their impact.

Information on cybersecurity threats are analysed, evaluated, synthesized information about potential security events, potential actors, attackers threatening security, and the methods and procedures they employ, which are used in cybersecurity risk management. While vulnerability-related information belongs to the "own/internal side" part of malicious security events, threat information belongs to the "attacker/external side".

The main types of *cooperation relationships between cybersecurity organizations* include:

- cooperation between a cybersecurity event management centre[14] and the cybersecurity operations centres (IT system operators) under its jurisdiction;
- cooperation between superior and subordinated cybersecurity event management centres with wider and narrower responsibilities (e.g. national and sectoral; or international, regional, federal and national organizations);
- cooperation between cybersecurity event management centres on the same level with non-overlapping responsibilities (e.g. different national or different sectoral organizations);
- cooperation between cybersecurity event management, or operations centres, and vendors of IT products;
- and finally, connections between cybersecurity event management, or operations centres, and military, law enforcement, or national security organizations.

The conditions for sharing cyber security information—within the legal framework—are determined by the information sharing policies of the individual organizations and the trust relations between the organizations.

The basic purpose of exchanging information between cybersecurity organizations is to enable each organization the access to information necessary to their decisions. For this purpose, it is necessary to share and provide information that is necessary and sufficient for the organization using the information. These are called "actionable information" by ENISA documents. [17: 2–4]

The role and significance of the ***interoperability of cyber security organizations*** is of paramount importance, as cybersecurity threats in global cyber space do not have organizational boundaries, and the network boundaries (even in case of distinct networks) are not impermeable. Although cybersecurity organizations sometimes produce new cybersecurity information, their activity is based on information, notifications, announcements, alerts, coming from outside the organization. Lack or lower level of interoperability means that organizations affected can only perform their activity with less information, or the processing of received information requires extra work, takes more time.

[14] Computer Security Incident Response Teams (in the EU), or Computer Emergency Response Teams (in the USA).

Technical level problems of interoperability are related to the data transmission (if necessary secure) links. Today these problems—apart from the potential problems of the secure connection—are relatively easy to solve. *Syntactic level problems* can occur during the exchange of unstructured (typically free text) data, related to the message formats used and the formats of each data element. The necessary transformations to solve these problems are also available, or feasible.

The *semantic level problems* in the field of cybersecurity are also a key issue for ensuring and maintain interoperability, and the provision of meaning-preserving information exchange. In this area there are a variety of taxonomies for different purposes, there are sets of controlled values sets, some of which are used in wider, others in a narrower scope of cooperation. In the future, it is expected that more cybersecurity classifications will remain in use, so their possible alignment or meaning-preserving transformations remain a task for actors involved.

Syntactic Level Interoperability Services for Cybersecurity

The meaning-preserving information exchange between the cooperating cybersecurity organizations—in order to resolve the existing differences—may require a number of syntactic level transformations. In the following, I will examine what types of syntactic level transformations may be required, and in which cases may they occur, and for what reasons the providing of this functionality occurs in the form of services provided by a third party.

The first group of syntactic transformations consists of ***transformations of data elements.*** Among these, the syntactic transformations of numeric, logical, date and time data are well formalized, algorithmised and can be solved on their own. In case of transformations of textual data (names, denominations, descriptions) between different character sets, formats (especially in case of names) and translations between languages the use of services may occur.

For systems that identify certain things (such as hardware or software components affected by security incidents or vulnerabilities) with names, the format for naming the same component may be different in two systems. For this reason, it may be necessary to convert from one format to another, or to split into a different number of name elements, or to make minor translations.[15] In case of textual descriptions, the necessity of translation does not need explanation.[16]

The implementation of these transformations in the form of a service may be justified by the wide, dynamically changing and expanding range of information, and expertise

[15] For example “Adobe Flash Player for Microsoft Edge és Internet Explorer 11 - 31.0.0.108 és korábbi verziói (Windows 10 és 8.1)” (govcert.hu, Hungarian Government Incident Response Team) ~ “Adobe Flash Player for Microsoft Edge and Internet Explorer 11” + “31.0.0.108 and earlier versions” + “Windows 10 and 8.1” (Adobe Security Bulletin)

[16] For example „A sérülékenységet a Cisco Umbrella API interfészéhez tartozó hitelesítés nem megfelelő konfigurációja okozza. Ezt kihasználva, egy hitelesített, távoli támadó olvashatja a saját és más szervezetek adatait, valamint módosítani is tudja azokat.” (govcert.hu) ~ “A vulnerability in the Cisco Umbrella API could allow an authenticated, remote attacker to view and modify data across their organization and other organizations.” (Cisco Security Advisory)

required (related to the formats used), the general nature of the task (machine translation), or the special domain knowledge related to translation of cybersecurity related texts.

The other group includes ***syntactic transformations between groups of data, and data structure representations.*** Basic tools for exchanging cybersecurity information are texts that meet simple structural and formal rules,[17] as well as XML and JSON formats. Transformations between these formats affect the parts describing the structure: in case of text, the order of components and the headings; and, in case of markup languages, the tags used. To transform the complete composite data format (representation), it is also necessary to convert data elements of the source format to data elements of the target format, which belongs to the previous set of transformations.

For transformations of groups of data, the source format may not contain all the required data for generating the target format, or contains data that is not included in the target format (are not of interest to the target user). The latter does not constitute an interoperability problem; it can be considered a realizable filtering that can be solved by the service. Missing data for syntactic level services in some cases may optionally be added, or the result will only be partial. This may be done by the omission of data, or using the “unknown” value. In case of mandatory data, successful transformation requires human, expert involvement. However, compared with a “manual” transformation, this can still be a very useful service.

One of the likely broadly useful services may be the transformation of the above-mentioned structured text data using a markup language (e.g. XML format) describing the structure and the type of data elements. The resulting format can now be further easily transformed to other, for example standard formats, or can be used to convert to a native, inner format of the cybersecurity actor’s IT system.

Semantic Level Interoperability Services for Cybersecurity

During the exchange of information between the cooperating cyber security actors, the most important and most difficult to resolve differences are the correct interpretations of the transmitted data. The features of cybersecurity events, vulnerabilities, threats, and other entities of interest are represented by all actors in a manner appropriate to their own goals and tasks.

Differences on the semantic level may, for example, appear in the parties’ classification of different things into a concept (e.g. what they consider as a security event); when things are categorized by different criteria, or with different details; the characteristics are described with different value sets; relationships between things are recognized differently. Much of these differences can be traced back to classifying and categorizing things, so I will focus on two questions of implementing transformations between different classifications.

Services performing the transformation between classifications can be implemented in “wired” form, using formalized conceptual systems, or in a complex way. In case of a *wired solution*, the party using the service must provide the source and destination classification identifier and the source classification value, and the service determines the classification

[17] For example the Hungarian Government Incident Response Team vulnerability list (database), or security bulletins, advisories, notifications provided by different organisations.

value according to the target classification. This solution can be used to convert between two specific classifications.

For *services based on formalized conceptual systems* (taxonomies, ontologies), the service provider implements the transformation with a general-purpose interpreter engine using semantic relationships (identity, is-a, etc.) between the classification values, as concepts. The advantage of this solution is that its capabilities can be expanded and improved by incorporating new classification concepts and conceptual relations without software modifications.

Using existing transformations between classifications, new *transformations built on successive steps* can be created. The disadvantage of this solution is that there may be a case in which there could be a one-to-one mapping between two classifications, but this is not possible through the intermediate classification (for example, because its detail is lower than that of the two others).

Organizations responsible for particular classifications can play a prominent role among ***service providers of transformations between cybersecurity classifications.*** They are able and even entitled to define the mapping in the most appropriate way between different versions of their classification systems. An example is the Top 10 vulnerability category system of the Open Web Application Security Project (OWASP), where there are four changes from 2013 to 2017.

An organization responsible for widely used detailed classification system may also be able to provide transformation from its own classification to a less detailed classification system. An example is the Common Weakness Enumeration (CWE) software security weakness categorization that is part of the US National Vulnerability Database, for which a mapping has been defined for different versions of OWASP Top 10 categories (2013, 2017).

Conclusion

The starting point for this publication is that the services provided by globally interconnected, decentralized IT systems and networks, the cyberspace, play a prominent role in our world. The dependence on these services requires the high-level security of cyberspace that can be ensured by a broad cooperation of different organizations, actors. Successful and efficient cooperation cannot be achieved without a similar level of information exchange between the actors, and their IT systems that requires interoperability of these systems.

Functionality ensuring interoperable information exchange between IT systems can be realized using own resources, or using services provided by third parties. The term interoperability service in the literature is described in several different forms, mostly without precise definition. The suggested definition of IT interoperability service is a service by which the service provider supports interoperable (meaning-preserving) data exchange between the information systems, tools and applications of service consumers, cooperating actors. Interoperability services can be implemented as middleware services, web services, and cloud-based services.

Interoperability services can be categorized according to different criteria: their level, nature, and availability. The benefits of using interoperability services are obvious, but there remain tasks that the service consumers (users) should do on their own. Interoperability service providers can be third party market-based providers, or internal providers, serving organizational, or cooperating community interests. Some interoperability services do not require application domain specific knowledge, but others (primarily on semantic level) do require.

Cybersecurity information exchange has special requirements for interoperability services. They require support for interoperable exchange of data about cybersecurity events, vulnerabilities, threats and other objects of interest. Syntactic level interoperability services can provide transformations of data elements, transformations between groups of data and data structures. Among semantic level interoperability services, the transformations between different classifications play an important role. Ideally, these can be provided by the organisations responsible for classifications.

References

[1] MUNK S.: *Katonai informatikai rendszerek interoperabilitásának aktuális hadtudományi kérdései.* (DSc-értekezés) Budapest: Magyar Tudományos Akadémia, 2007.

[2] MUNK S.: Az adaptív interoperabilitás fogalma és szükségessége katonai informatikai rendszerek esetében. *Bolyai Szemle,* 1 (2006), 28–39.

[3] MUNK S.: Changes in the military information interoperability environment. *Revista Academiei Forţelor Terestre,* 4 (2005), 39–51.

[4] WIEDERHOLD, G., GENESERETH, M.: The Conceptual Basis for Mediation Services. *IEEE Expert,* 5 (1997), 38–47. DOI: https://doi.org/10.1109/64.621227

[5] BUSSLER, C.: B2B and EAI with Business Process Management. In. CARDOSO, J., ALST, W. van der (eds.): *Handbook of Research on Business Process Modeling.* Hershey & New York: Information Science Reference, 2009. 384–402.

[6] CHARALABIDIS, Y., PANETTO, H., LOUKIS, E., MERTINS, K.: Interoperability Approaches for Enterprises and Administrations Worldwide. *The electronic journal for e-commerce tools and applications* (eJeta), 3 (2008), 1–10.

[7] LI, M. Sz., CABRAL, R., DOUMEINGTS, G., POPPLEWELL, K. (eds.): *Enterprise Interoperability, Research Roadmap Final Version (Version 4.0).* Information Society Technologies, 2006.

[8] *Content Management Interoperability Services (CMIS) Version 1.1 Plus Errata 01.* OASIS, 2015.

[9] *C3 Taxonomy Baseline 2.0* – AC/322-D(2016)0017 Enclosure 1, NATO Consultation, Command and Control Board, 2015.

[10] BISHOP, T. A., KARNE, R. K.: A survey of middleware. In. *Proceedings of the ISCA 18th Conference Computers and Their Applications.* Honolulu, 26–28 March 2003. 254–258.

[11] *Web Services Architecture.* W3C Working Group Note 11, 2004.

[12] *AC/322-D(2004)0040 Annex 1, NATO C3 System Interoperability Directive. Version 2.* NATO C3 Board, 2004.

[13] *Healthcare Gateway: Services.* https://healthcaregateway.co.uk/services/ (Downloaded: 05.10.2018)

[14] DESAI, P., SHETH, A. P., ANANTHARAM, P.: Semantic Gateway as a Service architecture for IoT Interoperability. In. *Proceedings of the 2015 IEEE International Conference on Mobile Services.* 313–319.

[15] MUNK S.: Kiberbiztonsági szervezetek közötti interoperábilis információcsere megoldások (sérülékenységek kezelése). *Bolyai Szemle,* 1 (2018), 54–77.

[16] MUNK S.: A kiberbiztonsági információcsere interoperabilitási kérdései. *Hadmérnök,* 3 (2018), 422–434.

[17] *Actionable Information for Security Incident Response.* Heraklion: European Union Agency for Network and Information Security, 2014.