SERVICE-ORIENTED CYBERSPACE FOR IMPROVING CYBERSECURITY

HENRYK KRAWCZYK

Faculty of Electronics, Telecommunication and Informatics
Center of Informatics, Tri-city Academic Supercomputer and networK
Gdańsk University of Technology
Narutowicza 11/12, 80–233 Gdańsk, Poland

(received: 28 January 2019; revised: 18 February 2019;
accepted: 25 February 2019; published online: 1 March 2019)

Abstract: The paper presents a cyberspace model where different categories of IT services are offered and used largely. A general cybersecurity policy is considered and the corresponding cybersecurity strategies are shown. The role of such technologies as: Internet of Things, Cloud Computing and Big Data is analyzed in order to improve the cybersecurity of a cyberspace. A new kind of service oriented cyberspace is proposed and its main properties are emphasized. Two simple examples of such cyberspaces are given and briefly discussed.

Keywords: cyberspace, key technologies, smart services, cybersecurity, policy and strategies
DOI: https://doi.org/10.17466/tq2019/23.2/d

1. Introduction

The technological and scientific progress has led to the creation and continuous improvement of real and virtual environments which support human life and human activities [1, 2]. In general, cyberspace is created and determined by the following issues:

- different kinds of data sources (devices, systems, platforms, people) which have obtained the data and information necessary to mine knowledge, allowing people and systems to take proper decisions;
- information systems and data processing platforms which allow us to process data, information, according to given algorithms to offer various kinds of IT services;
- access nodes of users which can perform and call various IT services to support human activities and to complement existing human services which are also available;

- general pointers of development trends observed in the space following from computer systems and common user activities, this is extra information, which can be used to make some changes in human decisions;
- telecommunication infrastructure that allows human communication, connection of various networks, steady and mobile devices (*e.g.* smartphones), network and application services, and also for data transition and for information exchanges;
- cybersecurity and trust mechanisms which provide the ability of the space to protect information and computer systems resources and telecommunication infrastructures, and also people; with respect to confidentiality, integrity, privacy, authentication, non-repudiation, *etc.*

Figure 1 illustrates the general idea of cyberspace. In practice we can distinguish different kinds of space. Taking into account geographical areas, we can distinguish such spaces as, for instance: city, region, nation or global world. Each of such spaces can differ in the level of digitalization and virtualization of their computing resources and services, and also in the means of telecommunication.

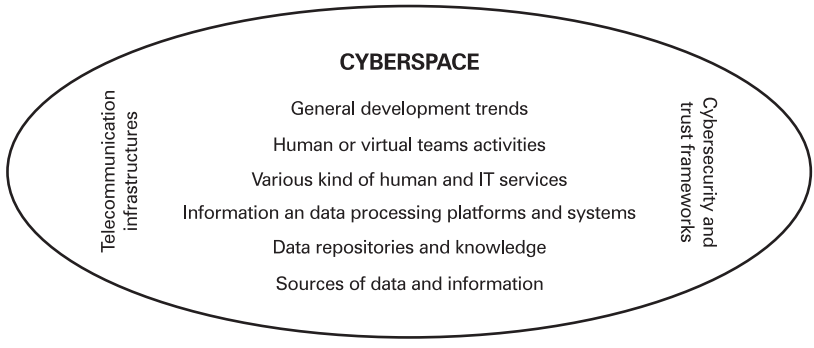

Figure 1. General idea of cyberspace

In addition to this, people in such spaces can distinguish their habits, activities or accepted values and attitudes. In accordance with this, different levels of cybersecurity can be recommended to be implemented to assure the assumed development directions. In other words, we can use a different cybersecurity policy to protect cyberspace, including a policy to bind the rights and duties of their inhabitants, to establish some cybersecurity frameworks, to express and develop those aspects that are wanted by those inhabitants [3, 4].

In consequence we can distinguish numerous categories of spaces according to the size of geographical regions. However, we can consider cybersecurity problems from the point of view of a much narrower domain. For each region, we can distinguish only such domains with high levels of digitalization and virtualization as e-transport, e-commerce, e-health or industry 4.0 [5]. A stick point of both classifications are IT services, which will be the main subject of our considerations.

It is assumed that technological innovations allow us to evolve and provide protective solutions. In Section 2 a general cybersecurity policy is considered, and the well-known cybersecurity strategies are mentioned. In Section 3 the role of key technologies, such as Internet of Things (IoT) [6], Cloud Computing (CC) [7] and Big Data (BD) [8] are presented and the main security problems are analyzed whereby a service-oriented cyberspace where all main functions are created by IT services implemented on different levels of functionality can be proposed. Such levels of digitalization and virtualization lead to the unification of cybersecurity problems. In consequence, it is easy to create cyberspaces with the required level of cybersecurity. Suggestions about the blockchain technology [9] are also included. Two examples of such cyberspaces with multilevel access control and with smart services are proposed and briefly discussed.

2. General cybersecurity policy and strategies

A cybersecurity policy is based on cybersecurity analysis of the given cyberspace tools, to create an appropriate cybersecurity architecture able to protect the cyberspace against threats and vulnerabilities and to minimize the effects of serious attacks. Figure 2 shows the main areas of each cybersecurity policy.

Serious cyber threats should be taken into consideration for cyberspace representing nations. These are as follows: malicious cyber activities, organized crime activities, pervasive technology imperfections, identity theft, denial of services, cyber espionage, *etc.* Then, the key tasks of any cybersecurity strategy (pillars) would be the following:

- protect government systems;
- create partnerships outside the habitat;
- protect citizens from cyberattacks;
- strengthen critical infrastructures;
- provide secure IT systems;
- develop security awareness for everyone.

To implement the above strategy different cybersecurity frameworks have been established for different sectors like government, military, critical infrastructure, health, transportation, *etc.* Such frameworks specify certain standards for protecting cybersecurity attributes such as: confidentiality, integrity, privacy.

Moreover, it is required to standardize the security requirements for different institutions, agencies and other form of activities in easier ways. Moreover, some service providers may offer specific functions related to attacks and volume abilities such as: Identify, Protect, Detect, Respond and Recover which facilitate the implementation of a cybersecurity architecture.

Each government is responsible for the preparation of a proper cybersecurity policy and an adequate cybersecurity strategy. The strategy should consist of one principle to support, on the one hand, values of fundamental freedoms, respect for property and privacy, and on the other hand, to fight cyberattacks

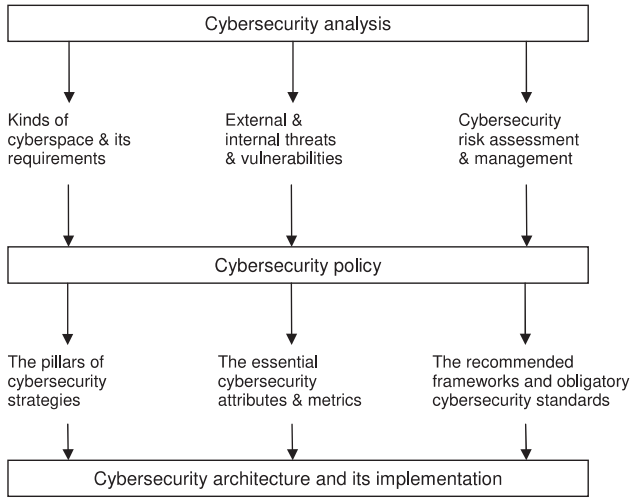

Figure 2. Main areas of cybersecurity policies

and cybercrime. Therefore, the strategy intends to provide a knowledge transfer to build cyber security: a best practice to enhance the ability to fight cyber-criminality, and to develop good relationships with the policy makers. The content of each national strategy varies according to the country structure and the needs of its inhabitants. However, the European Union prepared the EU's cybersecurity strategy called "An open space, Safe and Secure Cyberspace" which assumed five strategic priorities: achieving cyber resilience (framework ENISA – European Network and Information Security Agency), drastically reducing cybercrime, developing defense policies (CSDP – Common Security and Defense Policy), developing industrial and technological resources for cybersecurity, and establishing a coherent international cyberspace policy. In 2017 the EU's strategy was improved, and called "cybersecurity package in a nutshell", where three pillars were proposed: resilience, deference and defense, to build a strong single market in the area of cybersecurity. It means that the directive on the security of network and information systems (the NIS Directive) is the pattern for the EU legislation on cybersecurity, *i.e.*, a more effective law for criminal investigations and digital work without borders for cybersecurity strategy implementation and wide defense cooperation. Implementation of the strategy requires deeper engagement by all member states. They need to adopt a more strategic perspective but they have also some weak points (*e.g.* lack of the requisite expertise) and can prefer other (*e.g.* OECD) regulations for the IT infrastructure. However, building multilayer cyber-resilience requires reliable and trusting relationships between all participants. Looking beyond the EU, clear strategic guidelines for cyber foreign policy and credible links to decision making are becoming more important [10].

The important thing is that the EU invests a lot of money in cybersecurity development. For instance, the above cited subjects (*e.g.* Secure Societies – Protecting Freedom and Security of Europe and its citizens or Fighting Crime and

Terrorism) are included in the Horizon 2020 program, and some funds have been assigned to improving secure digital infrastructure, electronic identification, privacy and trust services (*e.g.* e-identification or interoperable health services) [11].

3. The technology triad

Implementation of cybersecurity architectures requires some serious understanding of the existing possibilities of today's essential technologies. In Figure 3 we show the coexistence of IoT (Internet of Things), Cloud Computing (CC) and Big Data (BD). They are still under development, consequently their significance is rapidly growing and they are changing cyberspace levels of digitalization and virtualization; and therefore, become more attractive for users. Besides, the 5G technology for building smart and efficient networks is also important to support the cyberspace functionality and human activities. In combination with other technologies they are creating new possibilities for building new kinds of IT services for users. Below, we limit our considerations to the IoT, CC and BD technologies only and show which new security problems should be solved to increase the cyberspace usability. It is important to explain the security issues of such a cyberspace and to develop new secure mechanisms of IoT, CC and BD which become the core components of next-generation application oriented systems.

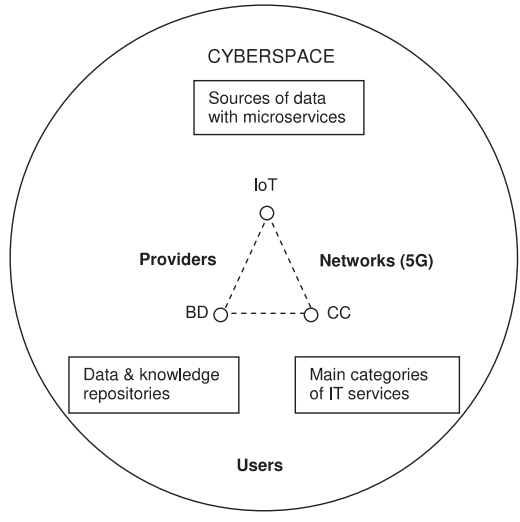

Figure 3. Coexistence of key technologies in cyberspace

3.1. Internet of Things

Development of embedded systems has led to the rise of the IoT technology. It evolved gradually from a single chip microcomputer, sensors, single board chips or industrial controllers, wearable devices to distributed microsystems, and then to ubiquitous and pervasive systems [12]. An IoT architecture consists of four layers, shown in Table t1. They are deployed in the open environment without protection

mechanisms; and their operations are simple without encryption and decryption calculations. Besides, they have multiple ways to access networks, hence, it is difficult to adopt the existing network protection and security mechanisms. Anyways, smartphones or different wearable devices have plenty of private data, which must be protected [13]. We distinguish different kinds of attacks at the computing or storage chips, to steal code, data or passwords, secret keys or other protection codes. Typical physical attacks cause the chip to be out of order (power) or have impact on the connectedness of channel information, processed data or execution instructions. Attacks on software can modify the code integrity (tampering), change the program running state (sabotage) and steal confidential data and privacy. In other words, attacks can be carried out on each layer separately or on arbitrary combinations of layers. Different security techniques to protect user privacy data (data distortion, encryption and anonymization) and to identify authentication of the communication protocols (endpoints, cross-domain or cross-networks domain). It is very important to consider the IoT architecture as a whole, and provide integrated and complete protections [14]. It is very important in quickly developing different smart environments, such as autonomous vehicles, smart cities, smart organizations or industry 4.0 with high security and safety levels [15].

Table 1. IoT layered-oriented architecture

Application Layers Platforms for implementation of different applications for different scenarios of management of process data providing quality service to users.
Middleware layer Providing more powerful computing (*e.g.* clouds and storage capabilities, databases, big data)
Network layer Wired and/or wireless data transmission medium, based on such technologies as: ZigBee, WiFi, Bluetooth, Cellular network technology 5G.
Perception Layer Identifying objects and collecting target information and transforming it into digital signals. Example: RFID tags, camera, sensors, wireless sensor networks to measure environmental conditions.

3.2. Cloud computing

CC is a distributed computing technology which has the advantage of multi-tenancy, on-demand customization, instant expansion and rapid configuration. A tenant is one of a group of users who share common access with specific privileges to the software instance. Customization depends on modification, and building personal specification or preferences, but configuration defines the way in which a computer system and a network system are set up and connected. Due

Table 2. Three main layers of computing cloud architectures

SaaS – Software as a Service
Uses the Web to deliver applications that are managed and maintained by third-party vendors and whose interfaces are accessed on the user sides. It does not require users to download or install and update the required software.
PaaS – Software as a Service
Allows customers to develop run and manage applications without building and maintaining the development infrastructure, and makes the development, testing and deployment processes quick, simple and cost effective.
IaaS – Infrastructure as a Service
Provides virtualized computing resources such as compute, storage and networking and self-service models for accessing, monitoring and managing remote infrastructures.

to virtual computing resources it provides remote users with IT services, through a distributed architecture (see Table t2).

We can distinguish three main categories of services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Each level uses different cloud resources. The suitable managing software (with a hypervisor) initiates the working of such hardware or software resources. IaaS makes available remote servers, storages and networks, which are monitored and controlled by software to achieve an acceptable level of computing performance. PaaS is responsible for access to development platforms to design and display software applications, which are run by users from clouds over the Internet or Intranet. The input and output data is collected in large-scale data centers, which are also available as other kinds of services. PaaS provides installation of different kinds of applications that are managed and maintained by third-party vendors.

The user interface of such applications is accessed on the user side. Professional tasks, such as computer or network configuration, management and maintenance belong to providers. Thus, large amounts of the user's prior investment in information-processing systems can be avoided, and in consequence, the cost of the use of information processing can be reduced.

Security problems of cloud computing platforms focus on four aspects such as: network security, virtualization security, data security and user privacy [16]. We can distinguish at least eight types of network security attacks: browser, brute force, denial of service, worm malware, Web scan and others. The most popular are browser attacks which attempt to breach a machine through a web browser. They often start at legitimate, but vulnerable websites, and infect them with malware. When new visitors arrive via such web browsers, the infected site attempts to force malware onto their systems, by exploiting vulnerabilities in their browsers. Next, brute force attacks try to discover the password for the system or service through trial and error. Denial of service attacks prevent legitimate users from accessing services or information. It succeeds when an attacker overloads server fire walls, e-mails with more requests than they can process. The main defense methods against denial attacks are: filtering attack

requests, which reduce cloud effectiveness, closing some blocked host parts and randomly releasing some host queues. Other attacks (SSL-secured Socket Layer) intercepts the data before it can be encrypted, giving the attacker access to sensitive data including credit card information and social security numbers. DNS spoofing occurs when data is introduced into the domain name system cache, causing the name server to return an incorrect IP address which redirects traffic to an alternate server. Anti-virus software firewalls and e-mail filters can ward off attacks and help manage unwanted traffic. Users can protect themselves by changing their passwords often, and by using odd combinations of numbers, letters and cases. Browser based attacks can be thwarted by regular updates of both browser and related applications.

Virtualization based security uses hardware virtualization features to create and isolate secure regions of memory from the formal operating system. It provides greatly increased protection from vulnerabilities in operating systems and prevents the use of malicious patterns which attempt to defeat protections. Such solutions require many system components (*e.g.* Trusted Platform Module) to be present and properly configured [12].

Data security refers to protective digital privacy measures that are applied to prove unauthorized access to servers, databases and websites. Extra mechanisms ensure that sensitive information is only disclosed to authorized parties (confidentiality which requires the use of encryption and encryption keys), prevent unauthorized modification of data (integrity) and guarantee that data can be accessed by authorized parties when requested (availability) [17].

User privacy security covers problems of how to collect, use, disclose, transfer and store personal data. Personal data relates to an identified or identifiable natural person, and concerns race, religion, sexual orientation and health. There are recommendations showing in what way it can be collected and processed.

The above security problems in cloud computing can be solved by a reinforcement technology, by deploying monitoring agent modules or ensuring the access request, and creating isolation between virtual machines. Furthermore, edge computing (the paths between data sources and cloud data centers) and fog computing (where cloud based services are closer to IoT devices in the edge networks) require a new security approach [18].

3.3. Big data

Big data is described by the 7V model where each V represents the data properties: volume (expressed in *e.g.* ZettaBytes), variability (changing of meaning), value (representing power in applications) variety (types of structured and unstructured data), velocity (speed of data growth), veracity (accuracy and dependability), visualization (the ways of presentation). According to different reports (*e.g.* CISCO, IBM) presently 2.5 quintillion pieces of data is generated per day, and this is set to explode to 40 yottabytes by 2020, which gives 5200 Gigabytes for every person on Earth. An important source of data is IoT, which comprises billions of devices such as sensors, medical apparatus, social networks,

Table 3. Big data layered architecture

Data consumption layer
Data mining for *e.g.* business and health processing – knowledge services Data oriented applications provided by third parties
Data analysis layer
Utilization of data analysis professional tools, or toolset design of new algorithms taking into account the 7V data model Creation of deep learning networks
Data messaging and storage layer
Conversion of unstructured data to the format understood by different tools, storing data either in RPBMS or in the Hadoop Distributed File System
Big data sources layer
IoT systems, database systems, mobile devices, sensors, e-mails, portals, enterprise apps, social media and networking sites, public profiles, government data

individual retrieves, smart cameras, software applications. In a nutshell, a large volume of veracity data is generated at high velocity from a variety of sources.

The cloud computing concept leads to virtualization of datacenter resources, and various types of data coming from applications, multitier Web, content delivery networks, and large-scale simulation can be rented on demand. This causes also the generation of plenty of data which can be written and read multiple times and further processed [19].

In a cloud, all user data is managed and maintained by cloud service providers. To protect user privacy all user data is encrypted, and then uploaded to a cloud storage service. However, cloud services cannot compute, statistically analyze, or retrieve cipher text, thereby affecting the quality of the service. It is also difficult to verify data integrity, because of HASH code functions, RSA homomorphism authentication algorithms must be used to confirm that the user who uploads data files is the owner of these files on the server. In consequence, different refried encryption algorithms are proposed and used to optimize cipher text retrieval [20].

Table t3 presents a big data layered architecture. It consists of four layers corresponding to data sources, storing data services, analyzing data services, and using data and knowledge services in data-oriented applications. According to the 7V model we can define challenges to big data security and privacy. Cloud-based storage has facilitated big data mining and collection, which has caused a challenge to determine new approaches of security check in the case of managing dynamic data, or continuous streaming data. Besides, in spite of scalability and availability new challenges are being posed to big data storage as the autotiering methods do not keep track of the data storage location.

End-point devices are the main factor for maintaining big data. Therefore, the provider should make sure to use an authentic and legitimate device on all layers of a big data architecture. It requires some new security protection mechanisms, particularly in the case of a distributed framework like the MapReduce

function of Hadoop. Similarly, due to large amounts of generated data, most providers are unable to maintain regular checks almost in real time. A prominent security flaw is that it is unable to encrypt data during a different group, when it is streamed or collected.

As the computing environment becomes cheaper, application platforms become networked, and system and analytics tools become shared over the cloud, security access control, compression and encryption and compliance introduce challenges that require systematic approaches, expressed as standards. The Cloud Security Alliance (CSA) Big Data Working Group has a mission to prepare such unified solutions [8].

In the future, big data architectures will become both more critical to secure, and more frequently attacked. This is the motivation of the emerging field of security intelligence which correlates security information across disparate domains to reach concrete conclusions. The first step is security analytics to detect not only new algorithms for intrusion detection or text understanding (log analysis) but also to cause that software and hardware developers become aware of many cybersecurity challenges. In other words, the design for cybersecurity is one of the promising branches of future research and practice.

4. Service oriented cyberspace

Service Oriented Architecture (SOA) is a standard based on loosely-coupled technology for connecting data, systems and even organizations. We distinguish three components of such architecture:

- service provider which is a company capable of providing IT services
- service requester which means users or companies that are in need of the IT services
- service broker which represents a company or a system that helps both the service provider and service requester to discover each other.

Three technologies are used to implement SOA and achieve standardized solutions: XML to present data, protocols or vocabulary, SOAP to be used for communication among different services, WSDL to describe functionalities of the services, and UDDI to publish and discover information about the services [21]. At the business level, a service can be viewed as a repeatable user task *e.g.*, (weather forecasting, paying with business cards). At the technical level it can be described by client interactions with various services, through messages according to the service specifications and service provider regulations. In general, loosely-coupled services reduce the vendor look-in and create a flexible infrastructure for distributed processing, which is used in many application areas. Besides, it can reduce the development and maintenance costs of various information processing systems.

Due to the SOA technology, the available functionality in a cyberspace can be expressed as a collection of services rather than a set of single applications. Then, the available multiple services can be aggregated into different applications. A developer can utilize the service orchestration to support the business process

automation by loosely coupling services across different applications and creating "second-generation" composite applications. In other words, new applications are created by a new orchestration of the existing services not by writing new codes. It is an attractive approach to creating a more agile and competitive system and reducing the time to market. Such a category of cyberspace will be called service oriented.

The natural evolution of an SOA are microservices [22] and nanoservices [23]. The terms "micro or nano" refer to the sizing of services. As the constituent services are small, they can be built by one or more small teams from the beginning, separated by service boundaries which make it easier to scale-up the development effort. Such micro and nanoservices also offer improved fault isolation: whereby, in the case of an error in one service, the whole application does not necessarily stop functioning. However, when the number of services increases, integration and managing of whole products can become complicated.

Microservices match well modern container management frameworks such as Kubernetes or Docker Swarm. They are widely used in today's distributed cloud-based service provisioning. These frameworks are not yet available in the embedded domain or in automotive systems, but are expected to be in the nearest future. Nanoservices, that are a miniature version of microservices, allow giving solutions for an autonomous service composition based on current needs. Locally composed services provide higher throughput and lower latency. Most of the sensitive data kept in a local computer can reduce the risks for security and privacy attacks. Lightweight virtualization technologies with a high number of nodes of IoT may be deployed for a single service, and we can assume that cyberspace is characterized by the available set of services, microservices and nanoservices. Then, security problems can be considered on such levels.

Cyberspace security can be defined as a state of freedom from risk and danger. Secure services means that their execution in cyberspace does not increase the risk and does not lead to any new danger. The main problem is to create services at the highest maturity level. It means to define and create services driven by business requirements, in business functionality terms, using some standards and optimize some quality metrics. The basic practices of engineering security in the service life cycle (from the design to the operation phase) are security planning, security requirement analysis of the security architecture design, security coding, security testing and security operation and maintenance. Each such practice encompasses specific methods, tools and techniques to design networks, distributed systems and applications. The World Wide Web Consortium (W3C) [24] has defined the Framework WSS (Web Service Security) standards, encompassing different specifications, each of them addressing specific aspects of security. There are seven specifications: WS-Security is intended to provide a message security model and the specification of mechanisms to attach signature and encryption leaders to the messages. WS-Policy describes the security policies, the mechanisms of trusted message exchanges. WS-Trust establishes both direct

brokered trust relationships. WS-Privacy proposes embedding the privacy language into WS-Policy and associating privacy claims with messages in WS-Security. WS-Secure Conversation extends the single message security provided by WS-Security to a conversation consisting of multiple exchanges. WS-Federation shows how to manage and broker trust relationships in a heterogeneous federated environment. WS-Authorization is supposed to provide support for the specification of authorization policies for managing authorization data.

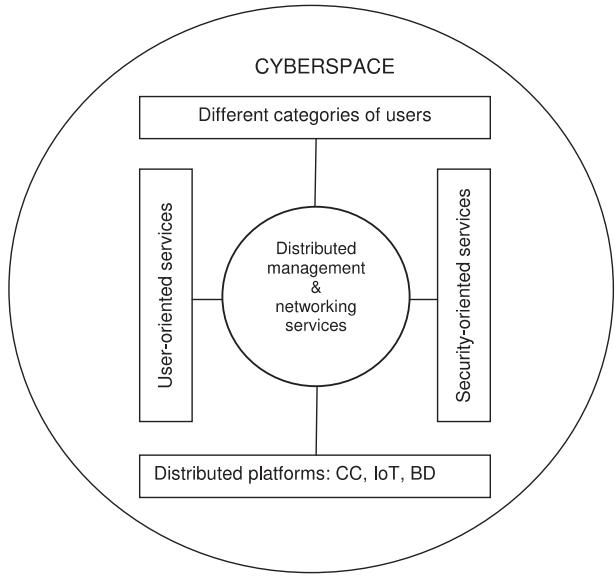

Figure 4. A simple model of service-oriented cyberspace

There are many examples of implementation of different kinds of secure services related to such systems as: e-health, e-commerce or smart houses. Today there are also many mature perimeter security technologies such as SSL (Secure Socket Layer) or encryption techniques used for data protection. SAML (Security Assertion Markup Language) describing a protocol for asserting, runtime checking, that is embedded in the execution environment, RASP (Runtime Application Self-Protection) used for authentication and authorization [25]. In consequence, some security services are available to support the cybersecurity of cyberspaces. They concern the user of services, platform referring services, transmitted data or messages. Authentication services verify that human users, registered system entities or their components, are who or what they claim to be. The availability services state the resources and services that should be available to authorized parties all the time (see the RBAC solution). Authorization Services ensure that only authorized principals may access and modify (change contents) resources. Confidentiality resources keep the message secret, by encrypting the messages in such a way that only authorized identities can decrypt and see the real data. The suitable cryptographic algorithms and protocols are used for protecting data and

messages from disclosure or modifications. Integrity services assure that every bit produced by the sender is received by the recipient in a precisely unaltered form. Finally, repudiation services prove that one identity has sent the data to another identity only, using the public key cryptography technology.

A simplified model of a secure cyberspace is shown in Figure 4. Users of such a space have at their disposal different kinds of services which are autocomplete with security services. Some network and management oriented services are also available to support the user – cyberspace cooperation. The design operations and management of such complex systems require the ability to describe them at various levels of abstraction, enabling analyses and decisions for technical, operational, management and business processes. It is computational interoperability that is required instead of data interoperability. It means consistent interpretation of the context, and the semantics, of operations or services in order to enable correct and resilient activities. An additional challenge in this direction is the integration of various technologies from purpose compacting, through communication and interfaces, to ownership and management. The distributed architecture of the cyberspace creates some timing problems specially for critical services. An extra response within a specific time interval is required to eliminate possible accidents. In addition to security, there is also a serious problem to eliminate dangerous incidents, distributed denial of service attacks, unreliable interaction with physical worlds, or sensitive information leakage and violating privacy rights. Therefore, special legal regulations and regulatory frameworks are required to protect against such incidents. Furthermore, an essential role in security assurance is played also by the liability of human operators, administrators and maintainers.

The active services in a cyberspace use various sets of data and need efficient mechanisms to guarantee data integrity. In general, such IT services are offered by third party cloud providers and special agreements between providers and users can be created and utilized in practice. It means that all user/provider central transactions can be manually managed which is time-consuming. To reduce this, blockchain mechanisms [9] are proposed and largely used in different cyberspaces. These blockchain mechanisms are ordered lists of blocks that contain transactions which cannot be deleted or altered without invalidating the chain. Programs deployed and run on a blockchain are called smart contracts and differ from service soft contracts, which cannot interact automatically between contractors. Such a new solution allows a design adaptable of blockchain-based systems which are considered to be used in many service oriented cyberspaces such as smart homes, smart cities, smart countries, and others.

5. Examples of service-oriented cyberspaces

Each service oriented cyberspace can be designed and implemented in different ways, taking into account the digitalization and virtualization levels (determined by nanoservices, microservices and services) as also by the security level requirements. Two examples of different cyberspaces are presented below,

where different security mechanisms are utilized. Figure 5 represents a cyberspace with multilevel access control. Such mechanisms are located in several places on different levels of the cyberspace. They are monitoring and controlling user access to the cyberspace, and also access to the required services and sources of data. A solution of such kind was implemented at the e-university platform (MyPG) working in the Gdańsk University of Technology. Intelligent access is achieved by controlled mechanisms which are much stronger if the trust to the user is lower, or if data is more sensitive. The current user trust level is estimated on-line basing on previous typical or unusual user behavior. It has been shown that the management time for such a solution is less time consuming [26], for nearly the same security level achieved in such cyberspace.

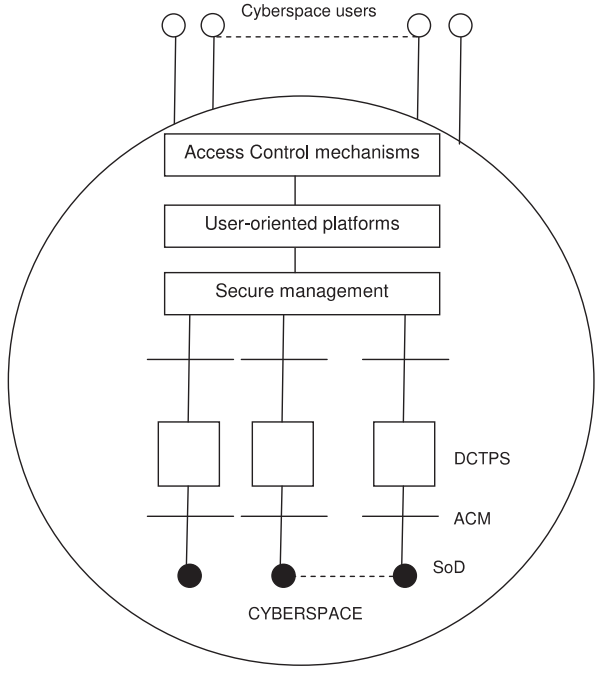

Figure 5. Cyberspace with multilevel access control

Figure 6 represents another kind of cybersecurity space, where so-called smart services are developed or improved. In this case we use transdisciplinary data coming from different categories of cyberspaces. It means that different data is monitored, but only special data is selected for further analysis. In this way the required knowledge is obtained in order to propose the suitable solutions for improving cybersecurity [27]. In a further step, the obtained knowledge is processed by different teams (virtual, real and virtual/real) to create new kinds

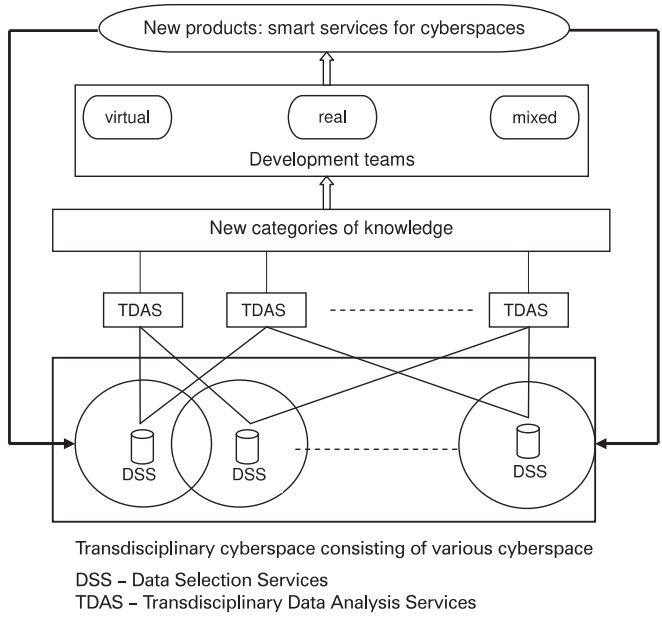

Figure 6. Transdisciplinary cyberspace for smart service design and improvement

of services. These services are called smart because they are: self-improving (s), maximum secure (m), analyzing big data (a), in real time (r), and using transdisciplinary data (t). Such kinds of services are planned to be developed in the Centre of Competence created together with the new building for the Centre of Informatics Tri-City Academic Supercomputer networK (CI TASK). This venture is funded by the European Union, and the main purpose is to create smart services for supporting research and development activities focused on university and business cooperation [27]. We hope than such an approach will also create new possibilities for improving the cybersecurity of inter- and transdisciplinary spaces where different kinds of smart services with high security and low risk are obtained.

6. Conclusions

The paper is focused on the creation of cyberspaces with the required level of cybersecurity. It is shown that it is possible for the so-called service-oriented cyberspaces. Such solutions are supported by three main technologies: IoT, CC and BD. The common idea is to determine a suitable set of IT services which would contribute to increasing the digitalization and virtualization levels. In consequence such services play a twofold role: they support the cyberspace functionality required by users, and also they contribute to the required cybersecurity solutions. It is also noted that the used technologies can create their own cybersecurity problems which should be eliminated in order to increase the level of cybersecurity. In the paper we present examples of such solutions. Moreover, one of the main

advantages of the proposed category of service-oriented cyberspaces is unification of cybersecurity problems which facilitates their analysis and leads to effective implementations, using for instance, such new techniques as the blockchain.

Taking into account cybersecurity management, two additional fundamental questions should be asked: what is the risk of intra- and extra-intrusion attacks for the space, and whether the cost of protection against such attacks is greater than the cost of recovering from them. Similarly, as for the digitalization and virtualization levels, the nature of the business is a key factor in determining the required level of security. This issue may be considered in future research.

References

[1] Curry E and Sheth A 2018 *Next-Generation Smart Environments: From System of Systems to Data Ecosystemsm, Internet of Things*, *IEEE Intelligent Systems* **33** (3) 28

[2] Serpanos D 2018 *The Cyber-Physical Systems Revolution*, *IEEE Computer* **51** (12) 70

[3] Goodwin C F and Nicholas J P 2013 *Developing a National strategy for CyberSecurity*, Foundation for Security Growth and Innovation

[4] Sabillon R, Cavaller V and Cano J 2016 *International Journal of Computer Science and Software Engineering (IJCSSE)* **5** (5) 67

[5] Caffey D Digital 2015 *Business and E-Commerce Management. Strategy, Implementation and Practice*, Marketing Insights Limited

[6] Rayes A and Salam S 2017 *Internet of Things – From Hype to Reality. The Road to Digitalization*, Springer

[7] Rittinghouse J W and Ransome J F 2016 *Cloud Computing, Implementation, Management and Security*, CRC Press

[8] Marz N and Warren J 2018 *Big Data: Principles and Best Practices of Scalable Realtime Data Systems*, Maming

[9] Manzor A, Braeken A, Liyanage M and Kanhere S S 2019 *Blockchain based Proxy Re-Encryption Scheme for Secure IoT Data Sharing* doi: 10.1109/BLOC.2019.3751336

[10] European Commission 2017 *EU Cybersecurity Initiatives working towards a more secure online environment*

[11] Caglayan M U 2019 *Some Current Cybersecurity Research in Europe*, *Security in Computer and Information Sciences* 9

[12] Esposito Ch, Castiglione A, Martini B and Choo K-K R 2016 *Cloud Manufacturing: Security, Privacy, and Forensic Concerns*, *IEEE Cloud Computing* **4** (4) 16 doi: 10.1109/MCC.2016.79

[13] Alioto M 2017 *IoT: Bird's Eye View, Megatrends and Perspectives, Enabling the Internet of Things*, Springer doi: 1007/978-3-319-51482-6_1

[14] Dawoud A, Shahristani S and Raun Ch. 2018 *Deep learning and software-defined networks: Towards secure IoT architecture*, *Internet of Things*, Springer doi: 10.1916/j.iot.2018.09.003

[15] Zalewski J 2019 *IoT Safety: State of the Art*, *IT Professional* **21** (1) 16 doi: 10.1109/MITP.2018.2883858

[16] CSA Research 2019 *Cloud Security*, alliance.org

[17] Wei D S L, Murugesan S, Kuo Sy-Yen, Naik K and Krizanc D 2013 *Enhancing Data Integrity and Privacy in the Cloud: An Agenda*, *IEEE Computer* **1** 87

[18] Zissis D and Lekkas D 2012 *Addressing cloud computing security issues, Future Generation Computer Systems* **28** (3) 583

[19] Henze M, Hermerschmidt L, Kerpen D, Häußling R, Rumpe B and Wehrle K 2016 *A comprehensive approach to privacy in the cloud-based Internet of Things*, *Future Generation Computer Systems* **56** 701

[20] Gorton I, Greenfield P, Szalay A and Williams R 2008 *Data-Intensive Computing in the 21st Century*, *IEEE Computer* **41** (4) 30
[21] Krawczyk H and Wielgus M 2006 *Security of Web Services*, *Int. Conf. Dependability of Computer Systems*, DepCos-Relcomex
[22] Sampaio Jr. A R, Rubin J, Beschastnikh I and Rosa N S 2019 *Journal of Internet Services and Applications* **10** 10
[23] Harjula E, Karhula P, Islam J, Leppänen T, Manzoor A, Liyanag M, Jagmohan Ch, Kumar T, Ahmad I and Ylianttila M 2019 *Decentralized IoT Edge Nanoservice Architecture for Future Gadget-Free Computing*, *IEEE Access* **7** 119856 doi: 10.1109/access.2019.2936714
[24] W3C Standards 2019, W3.org
[25] Bertino E, Martino L, Paci F and Squicciarni A 2010 *Secutity for Web Services and Service Oriented Architectures*, Springer
[26] Lubomski P and Krawczyk H 2017 *IEEE Security and Privacy Magazine* **15** 32
[27] Krawczyk H and Lubomski P 2017 *Task Quarterly* **21** (4) 299