Information & Security: An International Journal

G. Sharkov, v.37, 2017, 69-94 https://doi.org/10.11610/isij.3706

A SYSTEM-OF-SYSTEMS APPROACH TO CYBER SECURITY AND RESILIENCE

George SHARKOV

Abstract: To address the cybersecurity, safety, and reliability aspects of the entire digitalized ecosystems, we need first to understand and possibly model how the respective computer systems of different participating entities interoperate and collaborate. Modern computer systems and emerging applications are not just large-scale and complex in the digitally connected world. We categorize them also as decentralized, distributed, networked, interoperable compositions of heterogeneous and (semi)autonomous systems and/or elements. These new types of composite systems with emergent behavior have been defined as "Systems of Systems" (SoS). This paper explores different types of SoS and analyzes the interdependencies to manage cybersecurity threats and risks and achieve cyber resilience. We review various definitions and types of SoS and the application of SoS approach to situational awareness, threat intelligence, and composite risk assessment. An SoS view on managing the supply/value chain cyber risks is also outlined.

Keywords: system-of-systems, composite cyber risk, cyber threats, cyber risks, zero trust model, de-perimetrization, collaboration-oriented architecture, situational awareness, cyber picture, cyber resilience

Introduction

The pervasive and increasing digitalization of our industry, business, communication, public services, and our entire life rapidly transforms our society from technological through information, then knowledge-based, and finally, "cyber society." Digitalization means much more than the initial perception of computing and information technologies to "digitize" our world. While "digitization" commonly implies a shift from analog or physical to digital, "digitalization" is a complete digital transformation of business operations, models, and processes.[1] This significant shift is also considered a major driver of the fourth industrial revolution, or Industry 4.0. Digital infrastructures have become the backbone, or a fundamental critical factor, for the management and normal functioning of all resources and systems of national importance and governance of modern and democratic civil society. The citizens and the entire community rely on trustworthy and reliable information in the online virtual environment. Still,

they also expect trusted data sources, confidentiality and protection of personal data and their digital/virtual persona, along with adequate respect for human rights and liberties in cyberspace. Despite initial hesitation and concerns, states and politicians jump into the Internet to deliver information and services to citizens and businesses and for fast, almost instantaneous, transparent, and extensive contact with the community. Through e-Governance, states irreversibly migrate activities and services into digital-only form.

Although cyberspace provides virtually infinite opportunities for development to society and businesses, the growing and irreversible digital dependency generate new compelling risks and threats. The "knowledge economy" not only depends on but also introduces, with a longer-term perspective, unique aspects related to the intensive use of information systems, software management systems, and effective processes based on digital infrastructures. Supply chains (or, more generally - value chains) operate and deliver through the established virtual digital channels via their information systems and the Internet. Thus, the business risks expand with new "embedded" cyber threats of crucial importance, ignoring which would have catastrophic implications.

To address the cybersecurity, safety, and reliability aspects of the entire digitalized ecosystems, we need first to understand and possibly model how the respective information/computer systems of different participating entities interoperate. In the digitally connected world, modern computer systems and emerging applications are not just large-scale and complex. We categorize them also as decentralized, distributed, networked, interoperable compositions of heterogeneous and (semi)autonomous systems and/or elements. These new "composite systems" have been defined as "systems of systems" (SoS).[2] Systems engineers have used the term "System-of-Systems" (SoS) since the 1950s to describe systems that are "composed of independent constituent systems, which act jointly towards a common goal through the synergism between them."[3]

Most of the real systems of different scales and business areas today could be considered as a broader interpretation of the notion of SoS, such as the smart power grids, transport, manufacturing, logistics, supply chains, production, including military enterprises, and air traffic management. The IEEE Reliability Society has set up a special technical committee (TC) to assess the importance of the systems of systems approach for reliability and, more generally, dependability (RAMS: reliability, availability, maintainability, and safety).[4] It is also stressed that dependent and cascading failures are key aspects to be accounted for in system reliability, availability, and safety analyses. Thus, this approach is also the most suitable when studying and assessing the security and resilience of complex interoperable systems against cyber-

attacks or other disruptive and nefarious activities. This paper introduces a systematic SoS-based approach towards cyber risk assessment and management, operational incidents and threats management, prevention, and response. We describe the various layers of interoperability and dependability between systems, frequently addressed "above Layer 7".

Two novel aspects of SoS approach are also introduced. First, the interoperability layer between different security monitoring systems (like SIEMs, IPDS, or, more generally, Security Operations Centers), which not only perform info-sharing for the early warning but frequently perform active measures and changes in the local infrastructure or parametrization of the systems they continuously monitor. Then, at a higher level, another interoperable circle of anomaly-based behavior monitoring AI/ML/DL based systems are modeled as specific systems-of-intelligent-systems (SoIS). An illustration of the practical use of the SoS approach is given by applying it to supply/value chains for operational cyber risk management and identifying hidden threats and weaknesses.

Digitalized Ecosystems, Dependability and Interoperability

To understand the threats and cyber risks in a digitalized ecosystem, we need to assess the separate systems and subsystems and then the risks related to their interconnectivity and interoperability. The second group of emerging risks also has two aspects – on the one hand, they correspond to the nature of the dependencies between separate systems and the respective services they rely on each other, and on the other – on the reliability of the channels or interfaces through which these interdependencies are realized. These channels are of different natures and levels of abstraction and form the "layers" of cyberspace, or what is known as "cyber terrain." But first, let's start with the overview of the general digital dependency of our society and business due to digital transformation.

Digital Dependency and New Threats: If Software is "Eating" the World, Are we Safe?

Back in 2011, Mark Andreessen, the co-founder of Netscape, one of the first browser companies, and also a co-founder of the venture capital firm Andreessen-Horowitz and serial investor in most of the contemporary digital startups and fast-growing enterprises, stated that "Software is eating the world" in The Wall Street Journal article.[5] He said that "More and more major businesses and industries are being run on software and delivered as online services—from movies to agriculture to national defense." He argued that many of the Silicon Valley-style entrepreneurial technology companies are invading and overturning established industry structures, going com-

pletely virtual and digital by changing completely the business models or introducing new and innovative digitalized businesses. As meaningful examples, he gave Amazon, the largest bookseller, which is de-facto a software company. Also the largest video service by the number of subscribers, Netflix was a software company. Same with the dominant music companies – iTunes, Spotify, and Pandora. And to complete the picture – the fastest growing recruiting company was LinkedIn, and conservative sectors like healthcare, education, and national defense. He noticed that software was "eating" much of the value chain of industries that are widely viewed as primarily existing in the physical world – real-world retailers, even oil and gas companies. Finally, he predicted that the software would disrupt many more industries over the next ten years, with new world-beating Silicon Valley companies disrupting more cases than not. Finally, he shared his theory that "we are in the middle of a dramatic and broad technological and economic shift in which software companies are poised to take over large swathes of the economy."

Five years later, in 2016, Marc Andreessen returned by saying that software is not only "eating the world" but is already "programming the world."[6] As a continuation of the "software eating the world" thesis, he claimed that "all of a sudden, you can program the world." The ground for such a much stronger statement was in the new generation distributed systems, encompassing cloud and SaaS (Software as a Service), AI and machine/deep learning, and quantum computing, as well as the role of hardware, future interfaces, and data, big and small.

Cyberspace: Globally Interconnected and Interdependent Digitalized World

Marc Andreessen's statements point to one general conclusion: the digital transformation and massive digitalization or virtualization of our activities, business, and life, bring entirely new dependencies on complex business processes and information systems that control or mediate them. The driving new assets – information, including all types of data and digitalized knowledge, are entirely virtual and intangible, contrary to other physical assets. More generally, this new space we live and operate in has qualitatively new and different characteristics than the physical domains we know - land, sea, air, and space. Cyberspace also differs from other domains in that it is a constantly evolving and man-made construct with few limitations on where effects can be created. Being such a specific and different domain, cyberspace and our activities in it pose the question of sovereignty, governance, and defense, respectively. In 2014, in Wales, NATO allies declared this domain part of the environment we need to protect and defend, which is part of our societal sovereignty. Later, in 2016, at the Warsaw summit – as the fifth domain of military operations.

But how do we define "cyberspace," and is it a different domain? Most practitioners share a working concept of cyberspace as *"the collection of computing devices connected by networks in which electronic information is stored and utilized, and communication takes place,"* as the MIT expert David Clark defines it.[7]

Initially, the term "cyberspace" appeared in the 80s in the short story "Burning Chrome" (1982) by cyberpunk science fiction author William Gibson and later in his novel "Neuromancer" (1984).[8] But as Gibson said, when he coined it, "it seemed like an effective buzzword" to him. He didn't find any real semantic meaning, when he "saw it emerge on the page." Later, Don Slater used a metaphor to define cyberspace, describing it as a "sense of a social setting that exists purely within a space of representation and communication ... it exists entirely within a computer space, distributed across increasingly complex and fluid networks." In the 90s, the term "cyberspace" became a de-facto synonym for the Internet.

Cyberspace can be considered a global domain in the digitalized ecosystem consisting of interdependent networks of various IT infrastructures, including the Internet, telecommunications networks, different computer systems, industrial systems, embedded processors and controllers. Based on digitalized collaboration, cyberspace enables users to conduct business, connect, communicate, socialize, exchange information, knowledge, and ideas, play games and music, and interact in social forums.

Cyberspace can be represented as three layers with five types of interconnected and interoperable components, as follows:

- physical layer
    - geographic components
    - physical networks
- logical layer
    - logical network components
- social layer
    - cyber persona components (virtual world)
    - persona components (physical/social world).

This 3-layered model of cyberspace is also named "cyber terrain" and goes beyond the term "Internet," which is still frequently used as a synonym for cyberspace. While the physical layer components are mainly hardware components (infrastructure, wires/fiber, facilities, etc.), the logical layer provides both the channels and means of communication and data exchange (as data packets, routers, and other communication

devices with their respective system software). It also includes various systems and applications to process information, control the processes, and communicate at a higher semantic level. This layer is the mediator for the interconnectivity and interoperability between systems and devices. The social layer represents, on the one hand, the "actors" in the virtual environment (the cyber persona, the virtual persons acting in the digital space) and, on the other hand, the link to the real, physical world (physical persons, organizations, society). This layer provides the connection between the virtual and physical worlds. Business operations, organizations, services, and business processes run at that level, but through digital transformation, they are tightly coupled and supported by respective systems, applications, and communication channels of the logical layer.

On the other hand, to make that transition successful, helpful, and harmless, specific changes at the social layer are needed to meet the "logical" nature of the algorithms-based operations at the logical layer. Thus, the digital transformation would impose back to the social layer changes such as redefining the business processes and organization, ICT skills and competencies development, and in general, evolving the persona components to the highly demanding logical components. At a higher social level, it would require a change in organizational, national, and global strategies, policies, and measures to ensure the entire digitalized ecosystem's reliability, robustness, safety, and trustworthiness.

Understanding the Interconnectivity and Interoperability in Complex Systems

Since, at the logical layer, the activities are based on the intercommunication and collaboration between different systems at different levels (from info-sharing and data exchange to higher-level services and logical interdependencies), we need to study and understand how interoperability works. Following the popular SOA (Service Oriented Architectures) approach, and a proposed adaptation for SOA-based large-scale and distributed process applications, the levels of the conceptual interoperability model in support of integrability, interoperability, and composability for complex system-of-systems engineering, are defined as follows:[9]

- *Level 0:* Stand-alone systems have No Interoperability.
- *Level 1:* Technical Interoperability (data exchange via communication network protocols).
- *Level 2:* Syntactic Interoperability level introduces a common structure to exchange information.
- *Level 3:* If a common information exchange reference model is used, the level of Semantic Interoperability is reached.

- *Level 4:* Pragmatic Interoperability is reached when the interoperating systems are aware of the methods and procedures that others are employing.
- *Level 5:* Dynamic Interoperability - as a system operates on data over time, the state of that system will change, and this includes the assumptions and constraints that affect its data interchange. Systems are able to comprehend the state changes that occur in the assumptions and constraints that others are subject to over time and are able to take advantage of those changes.
- *Level 6:* Conceptual Interoperability - the highest level of interoperability. This requires that conceptual models be documented based on engineering methods enabling their interpretation and evaluation by other engineers.

Understanding the Interoperability in the Cyber Terrain: Beyond Layer 7

The SOA layers of interoperability described above represent mainly the technical or networked aspects of the interoperability, modeling complex enterprise systems. Another popular concept used to describe the design of a computer system designed to collaborate, or use services, from systems outside of your locus of control, is called Collaboration Oriented Architecture (COA). COA would typically utilize Service Oriented Architecture (SOA) to deliver the technical framework. Successful implementation of a COA requires the ability to successfully inter-work securely over the Internet and will typically face the problems that come with de-perimetrization. The key notions of COA and de-perimetrization and a guide for implementing such Secure Collaboration-Oriented Architectures (O-SCOA) were proposed by Jericho Forum in 2012.[10]

However, both models and architecture frameworks (SOA and COA) address the enterprise complex systems collaboration and interoperability. To understand the interdependencies in the real digitalized world, we need to consider a model much higher than the "application protocol layer" of inter-connectivity on which enterprise systems collaboration is based, known as "layer 7" of the OSI model (Open Systems Interconnection model).

To address the complete digitalized ecosystem or cyberspace, also named "cyber terrain," Shawn Riley [11] has described an immediately widely popular and comprehensive 15-layered model which integrates and defines much better the various types of components of the three-layer cyber terrain model above. The primary purpose of the proposed multilayered Cyber Terrain model is similar to the one of the traditional "terrain" maps. Namely, classic maps help users better understand the terrain and how to navigate the landscape. To apply this concept to cyberspace, we must first develop a detailed map. This cyber-map is the proposed multilayered cyber terrain model that allows us to model, organize conceptually, and understand the features (like laws,

policy, security technology, etc.) and the activities (cybercrime, APT, hacktivism, etc.) which take place in the cyber terrain. The Riley original multilayered map is shown in Figure 1, a copy from the original publication in 2014.

As it is observed in this 15-layered Riley model, it embeds the classical OSI (Open Systems Interconnection) model with layers from 2 to 7, and this forms the communication part of the logical layer from the 3-layer model. The physical and geographic layers mean the same as in the 3-layer model. The main difference and essential details given which help to understand how the systems and organizations interoperate at a higher logical and social level are above the layer 7. Here we will give a brief description of the layers, with some of the typical attacks illustrated by Riley for preparing the next chapter, related to threat hunting and risk analysis. The references are to CAPECs, Common Attack Patterns Enumeration and Classification, supported by the organization MITRE, along with the vulnerabilities and weaknesses enumerations, CVE and CWE, respectively.[12] The 15 layers of Riley are:

- *Layer 0:* Geographic Layer – the geographic area where real-world devices, people, organization buildings, and other physical items reside. It defines the context of the applicable cyber laws, policies, etc. It can represent geographic location attack vectors, such as leaving a few BadUSB infected USB thumb drives in the parking lot outside the office of a targeted organization. It also covers the risk from natural threats that affect the operations and people, such as earthquakes or flooding;

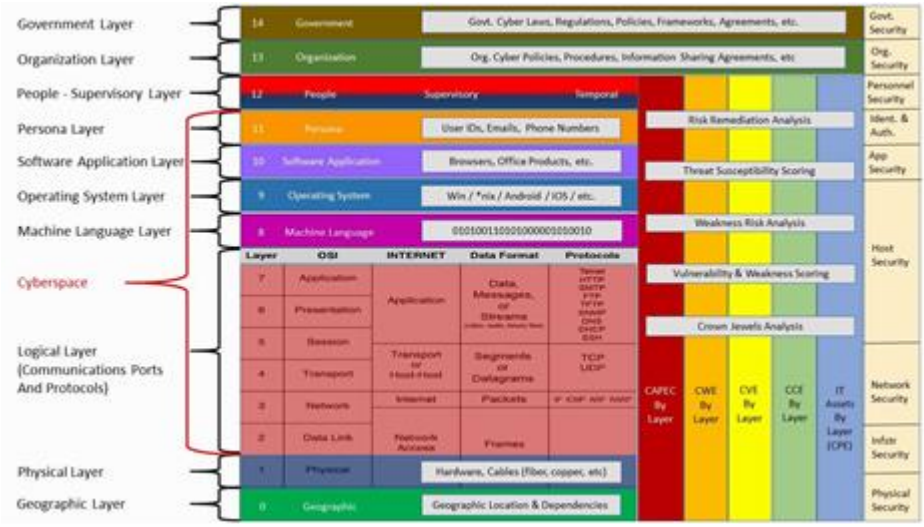

Figure 1: The original Cyber Terrain of Shawn Riley (2014) from analysis.blogspot [13]

- *Layer 1:* Physical Layer – the physical layer of the OSI model includes all the hardware, cables, etc. Respectively, this layer includes physical security and controlled access spaces. Examples of common attack patterns (CAPEC) at this layer: Physical Theft; Bypassing Physical Locks; Cloning Magnetic Strip Cards; Malicious Logic Insertion, etc.;
- *Layers 2 to 7:* Logical Layers – communications ports and protocols, i.e., the upper six layers of the standard OSI model covering communications ports and protocols of the cyber terrain. At this level, the list of CAPECs is the largest, as many indicators exist for compromise or malicious behavior, from specific packets observed in the network to port scanning and vulnerable software at the system level;
- *Layer 8:* Machine Language – used to represent data such as binary executables, class files, libraries (e.g., DLLs), or other machines' code. This includes items such as embedded systems, those used in SCADA, BIOS, and firmware on devices such as video cards and storage devices;
- *Layer 9:* Operating Systems – used to represent the operating systems used by the defender or the threat actor to include operation system weaknesses, vulnerabilities, security configuration issues, and attack patterns, such as B Buffer Overflow, Client-side Injection; Accessing or Modifying Executable Files, others;
- *Layer 10:* Software Applications – used to represent software applications installed across different operating systems. This includes the application code itself, but also the necessary application and service infrastructure used to support the application execution, such as web servers, .Net framework, OSGi, etc. These execution containers may also reveal critical information that could be used by adversaries to better understand an attack surface or leak information about the organization due to insecure configuration. This layer is also used to represent secure coding, software application configuration issues, vulnerabilities, weaknesses, and attack patterns. This is one of the most popular layers for attacks;
- *Layer 11:* Persona (or cyber persona) – user accounts, userIDs, email addresses, phone numbers, etc. This can include full credentials that allow access to information. A single person can have multiple persona identifies in cyberspace, a common tactic used by threat actors to better hide themselves;
- *Layer 12:* People / Supervisory / Temporal – real-world people (the actual individual). It includes attackers (like money mules, carders, botnet operators, APT actors) and defenders. Defenders also want to identify who the actual human person is behind the malicious activity for the purpose of prosecution, geolocation and other private data. Attack patterns involve variety of

social engineering techniques, Phishing (same applied to cyber persona, of course);

- *Layer 13:* Organization – organizational policies, processes, and procedures that apply to the defender's organization;
- *Layer 14:* Government – represent government items such as cyber laws, regulations, frameworks, and data. This layer can also represent alleged government associations of threat actors such as state-sponsored APTs.

The layers from 2 to 11 are usually referred to as "cyberspace," but the holistic approach to cybersecurity and resilience requires a complex multi-layer view with respective inter-layers dependencies. In addition, the SoS interoperability is based on patterns and activities that engage multiple layers as well (thus making the threats and vulnerabilities analysis complicated and based on composite and heterogeneous parameters). Attacks and defense (response) propagate and engage different layers, actors, channels and components, too.[14] This very detailed and comprehensive multi-layer model of Riley, in combination with the system-oriented models and architectures, provides the most widely applicable mechanism to identify, analyze and monitor the interdependencies between systems and processes, actors, and devices, through the various levels of networked communication channels. In addition, Riley added to the model what type of risk assessment could be performed at higher layers and linked it to asset management, vulnerabilities, and weaknesses analysis.

The SoS Approach to Global Connectivity and Interoperability

The 15-layers Riley model, described above, the anatomy of cyberspace and cyber terrain show the channels and "veins" through which the interaction and interoperability of actors, devices, and systems happen. But to model and analyze their active behavior and the dynamics of this interoperability, also considering the global connectivity, we need to employ some theoretical models of the system's research and collaborative systems architecture. Modern computer systems and emerging applications are not just large-scale and complex – we categorize them as decentralized, distributed, networked, interoperable compositions of heterogeneous and (semi-) autonomous systems and/or elements. The three basic types of collaborating and networked systems are shown in Figure 2.

These new "systems" are considered "systems of systems" (SoS).[15] The term "System of Systems" (SoS) has been used by systems engineers since the 1950s to describe systems that are "composed of independent constituent systems, which act jointly towards a common goal through the synergism between them."[16] Most of the real systems of different scale and business areas today could be considered as a wider inter-

pretation of the notion of SoS, such as the smart power grids, transport, manufacturing, logistics and supply chains, production, including military enterprises, and air traffic management.

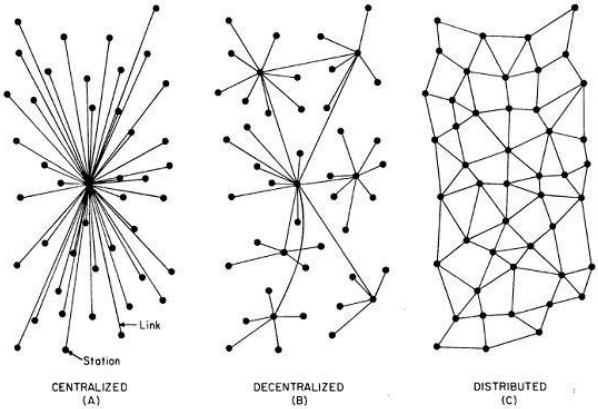

Figure 2: The three basic types of interconnected (networked) and interoperable systems.

Multiple definitions of the term "system-of-systems" (SoS) have been used since the first one from the 1950s and evolved following the complexity of cyber terrain and interoperability. The US standardization institute NIST considers that a *system of systems is a system whose elements are themselves systems, and these are referred to as "constituent systems."*[17]

Understanding the Dependencies and SoS Behavior

The SoS are not just complex systems or large-scale systems. According to Maier,[18] the characteristics of these new composite systems are:

- Operational Independence of Elements
- Managerial Independence of Elements
- Evolutionary Development
- Emergent Behavior
- Geographical Distribution of Elements.

In 2005, Daniel DeLaurentis [19] added three additional features of the SoS models and approach:

- Interdisciplinary Study
- Heterogeneity of Systems

- Networks of Systems.

The ISO/ICE defined SoS in the following way:

> A system of systems (SoS) brings together a set of systems for a task that none of the systems can accomplish on its own. Each constituent system keeps its own management, goals, and resources while coordinating within the SoS and adapting to meet SoS goals.[20]

Patterns for SoS Integration

The structure of SoS can be understood as an instance of a pattern.[21] System-of-systems patterns can be modeled at two layers: *operational* and *system*. At the *operational layer*, a variety of network topologies can be identified (see Figure 1 for the basic types). These include butterfly or bow-tie networks, in which one system (e.g., a common backbone) or a tight mesh of systems is central to all transactions, core-periphery type of networks, and mesh networks 9typical for distributed systems). From the viewpoint of security and reliability, all topologies are subject to attack propagation and cascading failures [22] in different ways and severity countermeasures. This propagation and cumulative cascading impact are also related to the dependencies at a systems level and the depth of coupling of systems and services (loose or tightly coupled).

At the *system layer*, interactions between constituent systems can be represented and analyzed from different technical viewpoints, depending on how constituent systems interact – via information exchange, behavior interaction or service use, complex behavior interaction or business logic, or a shared user interface. Five broad patterns of SoS architectures have been identified:

- centralized - corresponding to a butterfly or hub-and-spokes network
- service-oriented architecture (SOA)
- publisher-subscriber model;
- pipes-and-filters;
- blackboard.

Each of these system-level SoS architectural patterns needs to be adequately analyzed related to different possible adversary control strategies or attack patterns, as all they have strengths and weaknesses. Different patterns could be used for different purposes. As illustrated below and in Figures 3 and 4, functional or operations supporting SoS are typically of SOA, or COA (Collaboration Oriented Architecture) type, and “blackboard” or publisher-subscriber are widely used. For security and safety moni-

toring systems, critical resources control systems (say in ICS or SCADA systems), a more centralized approach is preferred. For Early Warning Systems, collaboration is essential, but due to the overwhelming information and alerts, a publisher-subscriber model is preferred.

Types of SoS

Regarding the types of SoS based on their interconnectivity and collaboration patterns, as presented by Bodeau et al. (2013),[23] the DoD (USA) Defense Acquisition Guidebook recognizes the following four SoS types:

- *Virtual SoS* – a virtual SoS lacks a central management authority and a centrally agreed upon purpose for the system-of-systems. Large-scale behavior emerges, and although it may be desirable, this type of SoS must rely upon relatively invisible mechanisms to maintain it.
- *Collaborative SoS* –in a collaborative SoS, the constituent systems interact more or less voluntarily to fulfill agreed upon central purposes. For example, the Internet is a "collaborative system". The central players collectively decide how to provide or deny service, thereby providing some means of enforcing and maintaining standards.
- *Acknowledged SoS* – an acknowledged SoS has recognized objectives, a designated manager, and resources for the SoS; however, the constituent systems retain their independent ownership, objectives, funding, and development and sustainment approaches.
- *Directed SoS* – a directed SoS is one in which the integrated SoS is built and managed to fulfill specific purposes. It is centrally managed during long-term operation to continue to fulfill those purposes as well as any new ones the system owners might wish to address. The constituent systems maintain an ability to operate independently, but their normal operational mode is subordinated to the centrally managed purpose.

Although the common internet-connected systems are of "virtual" or "collaborative" type, and the coupling there is mainly of loose type, in many specialized or dedicated collaboration groups (sub-networks, sometimes considered as deep-net) are of the type of "acknowledged" or "directed" and the coupling is stronger, also at a lower application protocols level. Therefore, the traditional approach and practices to build security depending on the different types of SoS were logically different. Most of the systems or SoS, considered as "closed" or air-gapped, typically of acknowledged or directed type, are designed based on the trusted and secure layers of communication and interoperability. This is proven by the practice as a very misleading and dangerous concept, and a new "zero trust model" is introduced, as discussed further below.

Addressing Threats and Risks in SoS

When we consider the operational running of complex interoperable systems-of-systems (SoS), we aim to establish and maintain an aggregated view from an operational perspective if all systems perform properly on their own and if the interoperability between them is smooth and performing well, thus hoping to achieve the basic view on the so-called "emergent behavior" of the SoS. However, the reality is that such complex systems are interlinked and interdependent at various and diverse layers, known as different levels of loosely coupling. A common mistake is to consider the coupling of systems as a binary value - either loosely coupled or tightly coupled. In reality, the granularity is diverse and somehow relative – some systems are more loosely coupled than others and allow larger flexibility and freedom in interoperating. Systems could be tightly coupled in one aspect and more loosely coupled in another.

The threats and risks in SoS are based on the vulnerabilities and weaknesses of the constituent systems plus the emergent weaknesses of their interoperability and dependencies both at the system and operational levels. Similar to the "emergent behavior" of the SoS, which is not the sum of the behaviors of the constituent systems, the overall risk is not just the sum or aggregation of separate systems risks. Therefore, a holistic approach to SoS risk management and threat intelligence needs to be established and applied.

Reliability of SoS

A consequence of the loose SoS architecture (loosely coupled ingredients of the compound systems) and interoperability directly affect the overall composite SoS reliability and security, such as: the possibility of dependent and cascading failures, complex event processing, chaotic behavior, scale-free phenomena, weak coupling, and weak signals. Since the "emergent behavior" of SoS capability, by definition, makes use of the capabilities of more than one constituent system to meet demand, then the SoS attributes emerge from the interaction of the constituent systems. Therefore, the SoS reliability is normally independent of the separate constituent systems reliabilities. The SoS might be more reliable than its constituents (because of better backup or redundant capabilities), or it could be less reliable (because of the weak information exchange and synchronization of processes). And, on the top of that, we should consider different configurations or states that will emerge dynamically in practice, including states and configurations that have neither been considered in the design phase nor tested, as all the systems evolve in practice. To address that, the IEEE Reliability Society has decided to set up a Technical Committee on systems of systems, to assess the importance of systems of systems for reliability and dependability (RAMS: Reliability, Availability, Maintainability and Safety).[24] Our goal is to

align with RAMS the cyber security and resilience view, as it maps logically to the principles of cyber/information security and resilience.

Building Trust: Towards Converged Security of SoS. Zero Trust Model

Considering the interdependencies, interconnectivity, and the layers at which they are performed in the SoS model, and respectively the new type of threats and risks, we need to reevaluate and certainly improve the approach to an integrated or "converged" security of the entire ecosystem. Based on the concept of a new, emergent behavior of the SoS, which is not the sum of the functionalities and behavior of the composite systems, we need to apply an adequate principle and a holistic approach to the security, safety, and reliability of the entire ecosystem.

Applying the Secure Coding Principles

A good starting point to approach the resultant security of interconnected and interoperable systems is to consider an extrapolation of the "Secure Coding" practices and principle, as addressed to the designers and developers of software and systems. Among the top 10 Secure Coding Practices, formulated by Robert Seacord [25] and also detailed in the various books and guides for secure coding (C, C++, Java, etc.), we should utilize at least the three, which are underlined and with some explanations in the list below:

1) *Validate input.* Validate input from all untrusted data sources. Proper input validation can eliminate the vast majority of software vulnerabilities. Be suspicious of most external data sources, including command line arguments, network interfaces, environmental variables, and user-controlled files.
2) Heed compiler warnings.
3) *Architect and design for security policies.* Create a software architecture and design your software to implement and enforce security policies. For example, if your system requires different privileges at different times, consider dividing the system into distinct intercommunicating subsystems, each with an appropriate privilege set.
4) Keep it simple.
5) Default deny.
6) Adhere to the principle of least privilege.
7) *Sanitize data sent to other systems*. Sanitize all data passed to complex subsystems such as command shells, relational databases, and commercial off-the-shelf (COTS) components.
8) *Practice defense in depth*. Manage risk with multiple defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of de-

fense can prevent a security flaw from becoming an exploitable vulnerability and/or limit the consequences of a successful exploit.

9) Use effective quality assurance techniques.
10) Adopt a secure coding standard.

The additional two practices – *"Define security requirements"* and *"Model threats"* are also relevant and applicable to SoS ideology.

It is obvious that "tightly coupled" SoS must comply with all the principles at all levels – from low level, direct calls or communication protocols to the highest level of the business logic interdependencies. A typical mistake would be to consider the "tightly coupled" services which run in controlled and protected environment and channels as isolated from the world. Typical for the air-gapped systems, like ICS/SCADA and security and defense IT systems. However, even for the "loose coupled" services al those principles are valid but need to be extrapolated and interpreted at policy and organizational level, rather than at technical level. This leads us to the newer model of interconnectivity, or the "Zero Trust Model".

Applying the "Zero Trust Model"

In 2010 the term "Zero Trust Model" was introduced by the analyst John Kindervag of Forrester Research to denote stricter cybersecurity programs and access control within corporations.[26] He suggested new basic concepts, architecture, and principles for network and information security, which are:

1) There are no longer a trusted and an untrusted interface on our security devices.
2) There are no longer a trusted and an untrusted network, and
3) There are no longer trusted and untrusted users.

Or shortly, all network traffic must be treated as "untrusted," and the concept of trust should not be applied to packets, network traffic, and data. Kindervag also stressed that malicious insider and insider threats would change the existing trust model. The "insider threat" concept has also changed the definition of the "parameter," or better said, invalidating the perimeter-based cyber defense idea. It also opened a completely new approach to cyber security, known as "de-perimetrization" in Collaboration Oriented Architecture (COA). In support of that, SEI (Carnegie Mellon) has developed a complete methodology for assessing insider threats, risks, and mitigation, among which the zero-trust principle about "no trusted and untrusted users" from above was widely elaborated. More recently, the "insider threat" concept, which initially addressed mainly people, evolved into "inside threat". This broader concept includes not only internal threat actors (users – physical/virtual persona - malicious, negligent,

or accidental/non-intentional) but also malware-infected (e.g., spyware, back door, ransom) devices or complete "zombie" machines. Although Kindervag was addressing the enterprise networks, all the principles are a valid, applicable, and perfect basis to approach the cyber security, reliability, and resilience of the system-of-systems.

Managing Cyber Security Risks. SoS for Collaborative Threat Intelligence.

From the security, reliability, and safety viewpoint, it is essential to transpose the natural loose coupling in different degrees (or levels) of dependencies. On the one hand, those dependencies need to be identified and assessed during the design phase to plan for proper risk management and develop respective monitoring and control tools. On the other hand, while operating, they have to be continuously monitored and evaluated from two perspectives – first, they will be used, intentionally or not, to propagate attacks, disruptions, or malfunctions of one system or component to the entire SoS ecosystem, and the second perspective – the dependencies themselves could be attacked or compromised, thus taking the entire ecosystem out of balance indirectly by tricking the context in which systems operate.

For illustration, in ICS/SCADA systems – one can imagine malware affecting and compromising the behavior of sensors, PLCs that would generate wrong data or perform incorrect actions, and through the properly functioning channels the central or intermediate levels of SCADA would be tricked. Alternatively – the SCADA main system (even only the HMI – human-machine interface dashboard itself) could be compromised, and all PLCs to function correctly while receiving improper commands based on the faulty central system and/or operator's decisions and actions. The second perspective is best illustrated by the man-in-the-middle (MITM) type of attack.

The threats and risks in SoS are based on the vulnerabilities and weaknesses of the constituent systems plus the emergent weaknesses of their interoperability and dependencies both at the system and operational levels. Based on the interdependencies and interoperability, we have two additional types of potential harms (impact) and respective risks due to the "synergy effect" or "cascade effect" of cyber incidents and campaigns. Another type of threat "hidden" within a longer chain of interoperability dependencies (for example, in a supply/value chain, see below) need to be considered, as they could have an unpredictable and unexpected massive "cascade effect."

The *synergy effect* we may define as seemingly independent or isolated incidents (like disruption or saturation of some services), and the leverage of the damage/harm is through the time frame and the accumulative effect. Let's not forget that in SoS the behavior of the entire ecosystem is not the "sum" of the separate functions or ser-

vices. In such case it would be essential to assess the impact based on higher-level dependencies (or loosely coupled services).

The *cascade effect* would be more observable when you have a logical dependency, and failure of one service would cause a propagating and possibly escalating impact over all connected and dependent services. This is mainly observed in strongly coupled systems. However, such dependencies are relatively easy to identify and systematically trace for preventive measures or monitoring in real time. Here the Big Data analytics help and including AI/ML methods for anomaly detection and thus eventually identifying wrong or dangerous data values on the run. In addition to the early warning systems of such an approach and prevention of the cascade effect, this continuous monitoring and validation of exchange data on both sides (sender and recipient side) would signal about the anomaly in a jeopardized system which is not directly observable by any SIEMs or SOCs locally.

SoS for Situational Awareness and Implementing Resiliency.

When evaluating and assessing the viability and resilient capabilities of complex, composite and adaptive systems such as the state with national governance and operational models, we need to go beyond the traditional risk-based approaches such as continuity of operations and disaster risk reduction processes. We need to develop augmented risk approaches that incorporate methodologies grounded in socio-ecological system resilience principles for improving the abilities to assess and manage both known and unknown risks. New models, such as Military Installation Resilience Assessment (MIRA) model,[27] apply risk and resilience principles to evaluate whole systems, focusing on interconnections and their functionality in facilitating response and adaptation. These principles and models are designed and applied successfully in complex organizational or enterprise systems, but the real challenge is to extend them to the higher, national level. At this complex level, we should consider models like system-of-systems which handle interconnectivities and dependencies that are not steady and fixed upon time. In practice, those complex and interconnected systems (actually, the backbones of the entire associated ecosystems) could be disrupted and turned to unpredictable and nondeterministic behavior though unthinkable scenarios, thus generating or opening unidentifiable and also unpredictable vulnerabilities which by nature would be easier exploitable with potential cascade or catastrophic effect.

Instead of over-engineering the risk management, the impact assessment should be based on the cost and consequences of failure of mission-related core services and operations of different organizations in the context of the entire ecosystem. Although various methods offer quantification of cyber-associated risks, still the major impact

of control and information systems disruptions or failures, data, and information breaches is largely difficult to quantify. Especially considering the prolonged hidden ("stealth") time, the APTs, sophistication, agility, and self-adaptiveness of campaigns with unrecoverable and unimaginable factors of damage in virtual or physical space.

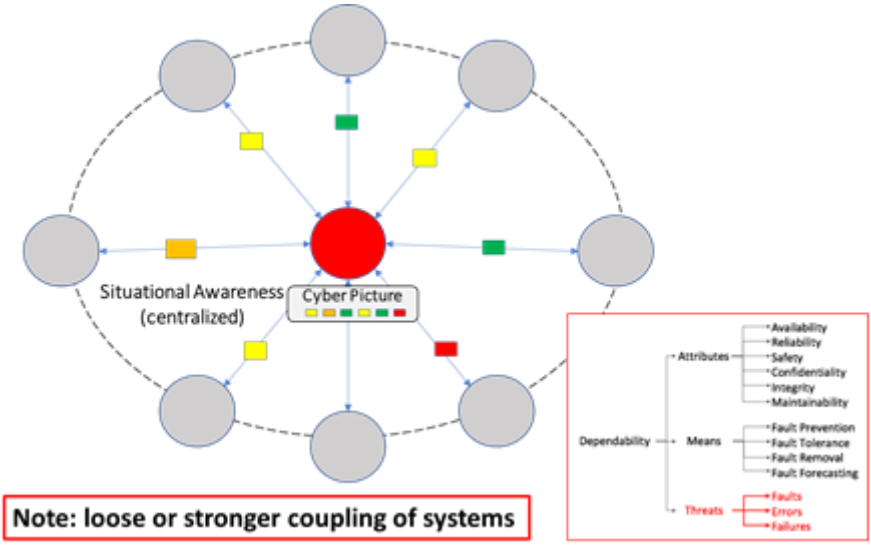

Figure 3: The "classical" scheme – decentralized "operational" SoS, but centralized "cyber picture" and SOC. Different types of dependencies and coupling are indicated.

The constituent systems in SoS, as well as the status of the interoperability between them should be continuously collected, aggregated, and analyzed to monitor the dynamic state of the SoS cyber terrain and evolution trends. The purpose is to provide an accurate and holistic representation of the domain (frequently referred to as *"cyber picture"*) which will support the decision making and responsive actions. As the distributed, and also typically decentralized or distributed systems (SoS) do not naturally expect to have a centralized joint monitoring and control SOC (or also "command center"), the cyber picture in SoS must be maintained in aggregated view but "broadcasted" to all players with respective details. The classical "centralized" view of the cyber picture and Soc is presented in Figure 3. We should note that the constituent systems may have loose or tight coupling, or mix, and be of a distributed type of connectivity for their standard business functions and services provided. However, the cyber picture and, eventually, the coordinated response would be centralized. This is

typical for many organizations (like banks, for example, or other critical infrastructure protection).

Further contributions add one more "+S" to RAMS for Security (RAMS+S).[28] Our approach also aligns with RAMS+S for SoS, the cyber security and resilience view of the compound system, as it maps logically to the principles of cyber/information security and resilience. It defines a new SoS interoperability and interdependencies "operations and security" layer on top of the SoS interoperability layer – we could name it Systems-of-Security-Operation-Centers (SoSOC). Similar to the new "emergent" behavior and capabilities of SoS, the SoSOC would have emergent capabilities, too. And they are also not just a sum of the separate ingredient Security Operations Centers (SOCs) capabilities and would also require collaboration which is much more than just info-sharing. The coupling among SOCs may follow the logic and degree of loose coupling of the underlined systems being monitored or may follow totally different logic (e.g., based on infrastructure, specific hardware or systems, geolocations, the sensitivity of the information, governance models, etc.). To sense the possible level of abstraction, one may consider this new SoSOC layer as an entirely "new world", to which the monitored systems and organizations are simply various data streams, but the "actions" might be cyber-physical and could vary from changing certain parameters to deploying Rapid Reaction Team (RRT) or switching to a resilience backup system/location. This new SoS-based approach to the organization of the Safety and Monitoring systems as a separate, relatively independent layer or sub-SoS of interoperability, and on top of the networked SOCs (or SIEMS) plus their functionality for early warning, threat mitigation, and coordinated response are illustrated in Figure 4. An indication of another new interoperable ring of specific systems is presented. Such new generation SoS interconnects the AI/ML empowered behavior monitoring systems of the constituents, which might be of two types – their regular operations and services or from the security perspective (thus empowering the SOC/SIEMs). Such AI-specific SoS will need further study and eventually new means for interoperability, as the major communication would be at a very high semantic level, but on the other hand, the constituent "intelligent" systems will have a "decision-making" power, especially for the autonomous or automatized processes.

SIEMs (SOCs) form an "intelligent" overlay or network but also have control and possible feedback to the systems being monitored. Because of that "community" of security agents and interconnectivity, info-sharing, predictive threat analysis, and

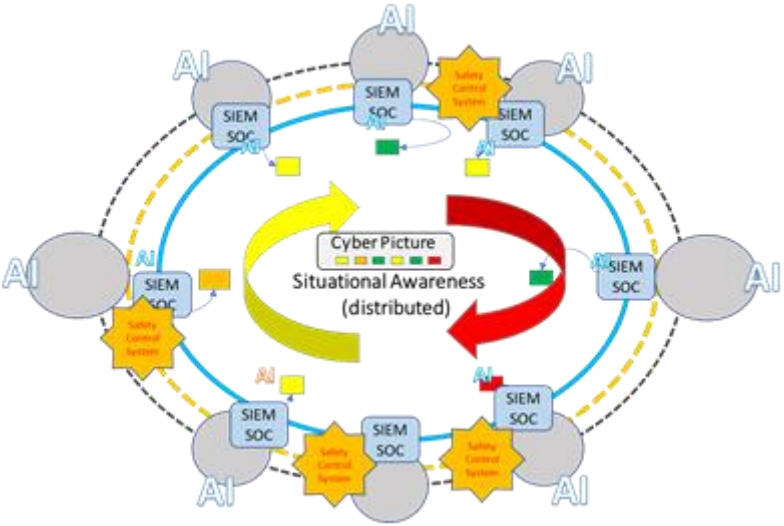

Figure 4: The advanced multi-SoS model with various SoS rings, or communities – traditional (functional) enterprise SoS, security overlay SoSOC (System-of-SOCs), and AI-empowered intelligent SoS.

measures, they could perform, sometimes automatically, on the systems being monitored and controlled. Thus, some modifications would be done, mainly in infrastructure configurations or network parametrization, that affect the behavior of the systems but not related to their function.

As a result of the complexity, heterogeneity, dynamically evolving composition and behavior of SoS, the threat landscape also continuously evolves, adding a lot of "unknowns." For the "knowns" (such as known vulnerabilities, exploits, even Zero-days, and advanced persistent threats – APTs), various detection and prevention tools can interoperate as well provide a large and diverse arsenal for "defense in depth." However, constantly some "hidden" vulnerabilities (sometimes "by design," like the Heartbleed and Spectre) appear and remind us that there are still a lot of "unknowns" which we won't be able to detect and prevent; thus, we need to build "resilience" of the entire SoS and have means to continuously monitor the integrity and interoperability.

SoS Approach to Supply/Value Chain Cyber Resilience

We consider SoS approach to achieve better security, trust and resilience of supply/value chains. First, we need to understand the interdependencies between the

agents and actors in a supply chain, and second – to evaluate how digital transformation brings their activities more and more on the cyber terrain. To do so, we need to start with the business model of the supply chains, or at a broader scope – the value chains. The best abstract and logical model, reflecting mainly the business dependencies, is the one proposed in 1985 by Michale Porter.[29] Value chains (or value streams) provide a logical scheme to identify and engage the interconnected businesses through their typical business dependencies, roles, and channels and then add the underlying digital dependency and the associated shared cyber risks. In addition, the value chains approach would allow joint and collaborative involvement and engagement of "small" and "big" businesses based on the natural business logic and clustering, not necessarily driven by ICT aspects. This allows the revealing various "hidden" threats and digital dependencies with significant potential impact on business continuity and resilience. There is no small or big in the value chain from a cyber security perspective – as "small" data breaches of essential data could jeopardize the entire chain. Moreover, within the chain, this would be of the type of "insider threat" but without means for forensics, intel, or other attribution techniques, a kind of "man in the business value chain." An increasing number of cases utilize weaknesses in aligning value chain business processes and practices and managing the interdependencies.

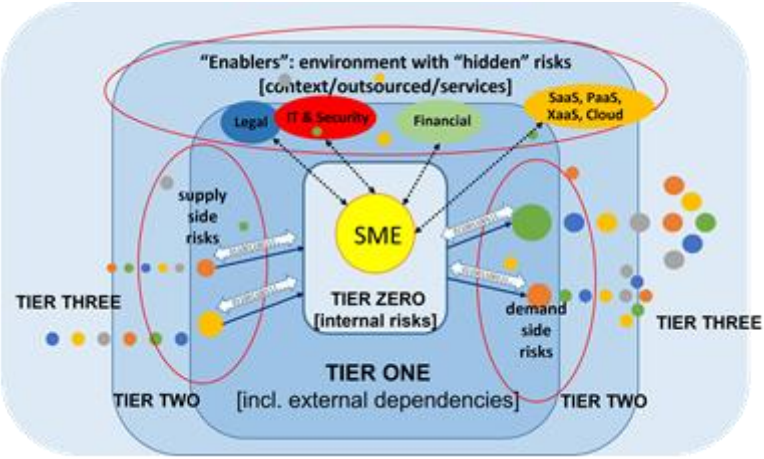

Figure 5: SoS view on the multi-tier supply/value with "enablers" and "hidden risks."

The complexity, interconnectivity, and multi-tier type of interoperability of the supply/value chains, plus the continuous digitalization of their operations and communication, made the SoS approach to their modeling, security risks management, and re-

silience applicable and with proven success.[30] The illustration of the value chain as SoS, with indication of the interdependencies on the main value stream, also mostly digitalized already, and the "enabler" parallel line are given in Figure 5.

The SoS approach helps to involve and engage all the actors in the supply/value chain by creating a chained and growing "appetite" of CEOs and leaders (including in small businesses, SMEs, on purpose indicated as a central business entity on Figure 5) for revealing cyber risks by exploiting the dependency chains, both on supply and demand side, but also including external services and dependencies (see the "Enablers" layer in Figure 5). The key to spreading such appetite, like a "good virus," is in sharing with first-tier partners (i.e., the first layer of connected businesses around the particular company), and this way, propagating the initiative through the connected business from both demand and supply side direction (method, derived from Social Network Analysis and combined with gamification techniques). Such gamified approach will pave the way for implementation and compliance with technical standards (such as ISO/IEC 27036). Value stream mapping was used to address also "insider threats" (this is "tier zero" in Figure 5). There are also risks at "tier one" shared with enablers and external services (providers of outsourced services, such as legal, payroll or bookkeeping, computer, and ICT maintenance, etc.).

Conclusions

The dramatically increasing complexity of the globally connected and electronically interoperable economy and society require an entirely new approach to mitigate the complex and frequently hidden risks emerging from digital dependencies. Handling the cybersecurity, safety, and reliability aspects of the entire digitalized ecosystems became unbearable without a holistic approach supported by relevant models and tools. Modern computer systems and emerging applications are not just large-scale and complex in the digitally connected world. Their interconnectivity is at different levels – data and info sharing, services, information, and knowledge sharing. The most important is that the business processes and logic of the business models and operations became so complex that the workflow is impossible to manage. We have presented and critically analyzed some aspects of the system-of-systems approach to this complex digitalized ecosystem. The goal is to achieve reliability, safety, and, most importantly, cybersecurity and resilience. By studying the anatomy of operations, interdependencies in cyberspace, and the connection to the real world, SoS help not only to model and manage, identify the composite threats and risks, and mitigate them. In other work, we have explained the SoS approach to establish a cybersecurity and resilience operational model at the national and international levels. We believe this approach is promising and applicable to different digitalized ecosystems – like

the supply/value chains, as we have briefly discussed, and at the higher level – cross-sectoral and national cybersecurity and cyber resilience.

References

1 "i-SCOOP: Digitization, digitalization, digital and transformation: the differences," accessed 1 July 2017, https://www.i-scoop.eu/digital-transformation/digitization-digitalization-digital-transformation-disruption/.

2 Mo Jamshidi, ed., *System of Systems Engineering: Innovations for the 21st Century* (New York: John Wiley & Sons, 2009).

3 Claus Ballegaard Nielsen, Peter Gorm Larsen, John Fitzgerald, Jim Woodcock, and Jan Peleska, "Systems of Systems Engineering: Basic Concepts, Model-Based Techniques, and Research Directions," *ACM Comput. Surv.* 48, no. 2, Article 18 (September 2015), https://doi.org/10.1145/2794381.

4 *Systems of Systems*, White paper, (IEEE Reliability Society, October 2014), accessed 1 July 2017, https://rs.ieee.org/technical-activities/technical-committees/systems-of-systems.html.

5 Marc Andreessen, "Why Software Is Eating the World," *The Wallstreet Journal*, accessed 1 April 2017, https://www.wsj.com/articles/SB10001424053111903480904576512250915629460.

6 Marc Andreessen and Ben Horowitz, "Software Programs the World" (a16z podcast, 12 July 2016), accessed 20 April 2017, https://future.com/podcasts/software-programs-the-world/.

7 David D.Clark, *Three views of cyberspace*, ECIR Working Paper No. 2011-1 (MIT Political Science Department, 2011), https://dspace.mit.edu/handle/1721.1/141694.

8 Scott Thil, "March 17, 1948: William Gibson, Father of Cyberspace," *WIRED* March 17, 2009, https://www.wired.com/science/discoveries/news/2009/03/dayintech_0317.

9 Robert Harrison, et al., "Next Generation of Engineering Methods and Tools for SOA-Based Large-Scale and Distributed Process Applications," in: Colombo, Armando et al. (ed.) *Industrial Cloud-Based Cyber-Physical Systems* (Springer, Cham, 2014), https://doi.org/10.1007/978-3-319-05624-1_6.

10 Jericho Forum, "Framework for Secure Collaboration-Oriented Architectures (O-SCOA)" (Open Group, 2012), accessed July 30, 2017, https://publications.opengroup.org/g127.

11 Shawn Riley, "Cyber Terrain: A Model for Increased Understanding of Cyber Activity," Blogspot article, October 7, 2014, accessed 30 April 2017, http://cyber-analysis.blogspot.com/2014/10/cyber-terrain-model-for-increased.html.

12 MITRE, "CAPEC (Common Attack Pattern Enumerations and Classifications)," https://capec.mitre.org/.

13 Shawn Riley, "Cyber Terrain."

[14] David Raymond, Gregory Conti, Tom Cross, and Michael Nowatkowski, "Key Terrain in Cyberspace: Seeking the High Ground," in: P. Brangetto, M. Maybaum, J. Stinissen, eds, *6th International Conference on Cyber Conflict* (Tallinn: NATO CCD COE Publications, 2014), 287-300.

[15] Mohammad Jamshid, ed., *System of Systems Engineering: Innovations for the 21st Century* (New York: John Wiley & Sons, 2009).

[16] Claus Ballegaard Nielsen, Peter Gorm Larsen, John Fitzgerald, Jim Woodcock, Jan Peleska, "Systems of Systems Engineering: Basic Concepts, Model-Based Techniques, and Research Directions," *ACM Comput. Surv.* 48, no. 2 (September 2015), article 18, https://doi.org/10.1145/2794381.

[17] NIST, "NIST SP 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," NIST SP 800-160, November 15, 2016.

[18] Mark W. Maier, "Architecting Principles for Systems of Systems," *Systems Engineering* 1, no. 4 (1998): 267-284, https://doi.org/10.1002/(SICI)1520-6858(1998)1:4%3C267::AID-SYS3%3E3.0.CO;2-D.

[19] Daniel DeLaurentis, "Understanding Transportation as a System-of-Systems Design Problem", in *43rd AIAA Aerospace Sciences Meeting and Exhibit*, 2005, https://doi.org/10.2514/6.2005-123.

[20] ISO, "ISO/IEC JTC 1/SC 7, ISO/IEC/IEEE 15288:2015 - Systems and software engineering – System life cycle processes," International Organization for Standarization, 2015.

[21] Rick Kazman, Klaus Schmid, Claus Ballegaard Nielsen, and John Klein, "Understanding patterns for system of systems integration," *2013 8th International Conference on System of Systems Engineering*, 2013, pp. 141-146, https://doi.org/10.1109/SYSoSE.2013.6575257.

[22] Tarik Roukny, Hugues Bersini, Hudues Pirotte, Guido Caldarelli and Stefano Battiston, "Default Cascades in Complex Networks: Topology and Systemic Risk," *Scientific Reports* 3, *A Nature Journal* (September 26, 2013), accessed 1 June 2017, https://www.nature.com/articles/srep02759.

[23] Deborah Bodeau, John Brtis, Richard Graubart, and Jonathan Salwen, "Resiliency Techniques for System of Systems: Extending and Applying the Cyber Resiliency Engineering Framework to the Space Domain," MITRE, MTR 130515, PR 13-3513, September 2013, http://www.mitre.org/sites/default/files/publications/13-3513-ResiliencyTechniques_0.pdf.

[24] System of Systems, IEEE.

[25] Robert Seacord, "Top 10 Secure Coding Practices," CERT/SEI Secure Coding, https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices.

[26] John Kindervag, "Build Security into Your Network's DNA: The Zero Trust Network Architecture" *Forrester Research* 5 (November 2010), accessed 22

January 2017, https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf.

[27] Nicole Sikula, James Mancillas, Igor Linkov, and John McDonagh, "Risk management is not enough: a conceptual model for resilience and adaptation-based vulnerability assessments," *Environ Systems and Decisions* 35 (2015): 219-228, https://doi.org/10.1007/s10669-015-9552-7.

[28] Jochen Link, Karl Waedt, Ines Ben Zid, and Xinxin Lou, "Current Challenges of the Joint Consideration of Functional Safety & Cyber Security, Their Interoperability and Impact on Organizations: How to Manage RAMS + S (Reliability Availability Maintainability Safety + Security)," *2018 12th International Conference on Reliability, Maintainability, and Safety (ICRMS), Shanghai, China,* 2018, pp. 185-191.

[29] Michael Porter, *The Competitive Advantage: Creating and Sustaining Superior Performance* (New York, NY: Free Press, 1985).

[30] Tsan-Ming Choi, "Managing service supply chains in the big data era: a system of systems perspective," in *Service Supply Chain Systems: A Systems Engineering Approach*, edited by T.M. Choi (London: CRC Press, 2016), 73-80.

About the Author

Dr. George Sharkov is CEO of the European Software Institute CEE since 2003 and Head of the Cybersecurity Lab at Sofia Tech Park. He is adviser to the Bulgarian Minister of Defense (since 2014) and National Cybersecurity Coordinator, leading the national Cyber Resilience Strategy development. Member of the EU AI High Level Expert Group, and SMEs voice at ETSI Technical Committees CYBER. He holds PhD in AI and is lecturing at four leading universities (software quality, cybersecurity and resilience, and active security). *E-mail:* gesha@esicenter.bg