future internet

Review

Review on Semantic Modeling and Simulation of Cybersecurity and Interoperability on the Internet of Underwater Things

Konstantinos Kotis *, Stavros Stavrinos and Christos Kalloniatis

Department of Cultural Technology and Communication, University of the Aegean, University Hill, 81100 Mytilene, Greece
* Correspondence: kotis@aegean.gr; Tel.: +30-69-7482-2712

Abstract: As maritime and military missions become more and more complex and multifactorial over the years, there has been a high interest in the research and development of (autonomous) unmanned underwater vehicles (UUVs). Latest efforts concern the modeling and simulation of UUVs' collaboration in swarm formations, towards obtaining deeper insights related to the critical issues of cybersecurity and interoperability. The research topics, which are constantly emerging in this domain, are closely related to the communication, interoperability, and secure operation of UUVs, as well as to the volume, velocity, variety, and veracity of data transmitted in low bit-rate due to the medium, i.e., the water. This paper reports on specific research topics in the domain of UUVs, emphasizing interoperability and cybersecurity in swarms of UUVs in a military/search-and-rescue setting. The goal of this work is two-fold: a) to review existing methods and tools of semantic modeling and simulation for cybersecurity and interoperability on the Internet of Underwater Things (IoUT), b) to highlight open issues and challenges, towards developing a novel simulation approach to effectively support critical and life-saving decision-making of commanders of military and search-and-rescue operations.

Keywords: IoUT; UUVs; swarm; interoperability; semantics; cybersecurity; simulation

check for updates

Citation: Kotis, K.; Stavrinos, S.; Kalloniatis, C. Review on Semantic Modeling and Simulation of Cybersecurity and Interoperability on the Internet of Underwater Things. *Future Internet* **2023**, *15*, 11. https://doi.org/10.3390/fi15010011

Academic Editor: Wei Yu

Received: 21 November 2022
Revised: 17 December 2022
Accepted: 23 December 2022
Published: 26 December 2022

1. Introduction

Technology for maritime and military missions nowadays is demonstrating a rapid development in different directions such as high distance tracking radar, the integration of heterogeneous systems for improving operational time and the cooperation with air and sea. Costly, uncertain, and dangerous operations such as search-and-rescue (SAR) or hydrography and ocean floor mapping, are now performed in few hours instead of days/months, in a cost-efficient manner, minimizing human involvement. On the other hand, assigning highly risky (and usually deadly) missions to humans, raises ethical concerns since prioritization and importance of human lives is undeniable. In addition, the cost of such operations is enormous, mainly due to the energy and fuel consumption of involved systems/platforms. Planning such operations must seriously consider the cost-efficiency factor, especially when combined with time and cost needed to repair damaged air, surface, or subsurface vehicles. A key solution for this challenge is the use of autonomous and unmanned vehicles, which are self-managing, cost-efficient, and effective in accomplishing several highly risky and resource-demanding tasks. As a result, unmanned vehicle systems/platforms below and above the water, and in the air, have become a priority of military and non-military industries.

In the last decade, the interest in unmanned underwater vehicles has been increasing. The North Atlantic Treaty Organization (NATO), in collaboration with academia, have developed distinct sectors for exclusive research related to this topic. Unmanned or autonomous underwater vehicles (UUVs/AUVs), namely drones, and remotely operated vehicles (ROVs), have been developed for years. There are several differences between them, with the most fundamental being the human factor. UUVs/AUVs demonstrate some form of intelligence, planning their own path, without exclusively depending on humans, acting completely autonomously most of the time. ROVs, on the other hand, depend on a remote human operator, and, as a result, many restrictions in their usage are emerging. Both UUVs/AUVs and ROVs, usually operate in an underwater wireless sensor network (UWSN). This type of network supports the monitoring of the aquatic environment and the wireless bidirectional transmission of data between users, i.e., underwater vehicles. This paper's focus is on UUVs/AUVs.

UUVs/AUVs are considered today a powerful scientific and military "tool" which, when operating in swarm formations, achieve tremendous goals. A swarm of UUVs concerns multiple UUVs that can interoperate, communicate, and behave as a unit. Ideally, one of the UUVs is the leader, having the main decision-making role. Several sub-groups with leaders could also exist. Every unit in the swarm should have the permission and ability to take leadership in situations where the leader is unable to operate efficiently (for any reason, e.g., circuits' damage). The operation of UUVs in a swarm is a powerful platform that provides huge capabilities towards a successful operation (military, scientific, other), even in risky and hazardous settings, putting aside any ethical doubts of a human (e.g., military commander, chief scientist), especially when the full-autonomous decision-making loop for the leader is achieved. Semantic knowledge and ontologies are key solutions to achieve successful interoperability in a swarm of UUVs, ensuring all the above requirements. Whatever the mission/operation, UUVs/AUVs can support it efficiently, either in civilian or in naval SAR and military operations. For example, the AUV A18D of ECA GROUP (https://www.ecagroup.com/en/solutions/a18-d-auv-autonomous-underwater-vehicle, accessed on 20 November 2022) achieved the precise mapping of the seabed at a depth of 3000 m in the strong currents of Atlantic; it also efficiently detected various debris and wrecks [1]. Furthermore, AUVs supported a huge operation surrounding a plane crash (Air France Flight 447), discovering pieces of the plane and its "black box" with side-scan sonar [2]. Finally, Knifefish of the US Navy fleet can detect and classify mines in large depths of the underwater environment with high clutter [3]. NATO is integrating UUVs in their fleet gradually, trying to counter several challenges.

An important, still open, issue in this domain of research is interoperability. Most of the systems/platforms that NATO is using, as well as the ones developed by research institutes, follow their own standards and protocols for command, communication, and control, creating the obvious need for interoperability via a cross-platform approach. In addition, the water, as an environment for data transmission between UUVs, raises another prominent issue, i.e., the security of underwater networks. More specifically, cybersecurity assessment and security updates should be a continuous concern, along with the data sender/receiver authentication. In the era of big data and the Internet of Things (IoT), the volume (sensor) data that is created and exchanged in a communication network is, at least, voluminous. Moreover, the data exchanged in this context have more characteristics, referred to as the four Vs, i.e., volume, variety, velocity, and veracity [4]. Considering that the exchange of big data between various heterogeneous underwater/surface/air systems/platforms should be performed in real-time, this process, when performed in a medium of transmission with extremely low bitrate (i.e., in the water) and with several physical phenomena influencing the quality of transmission, is considered highly unsafe. The principal concern of latency in safe communications, is the delay in (re)distributing a vast number of data packets, to evaluate alerts from cyber-incidents and consequently to counter them. Moreover, due to the volume of exchanging information, recurrence of the same data is another deterrent issue which is encountered, along with "sieving" these data, decongesting the underwater network and accelerating the quality of the transmitted information.

Let us assume the following SAR scenario (Figure 1). A swarm of UUVs must travel to the location of a plane crash at sea, safely and quickly, while interoperating in an underwater sensor network (UWSN), exchanging information/data in real-time, utilizing adaptive path-planning. During the execution of their assigned tasks, an unusual delay in communication between them and with the underwater nodes is identified, affecting the robustness of the network architecture, resulting in the inability to receive information from the commander. An automated analysis of the incident issues an alert for huge numbers of packets, overwhelming the network, thus, an incoming DoS (denial of service) attack is flagged. Consequently, an automated process of various counter-measures methods and protocols is initiated, such as honeypots, encryption algorithms, security rules, etc. For training and anticipation optimization, such a scenario must be simulated for commanders, developing a simulation tool always available for consulting and training, validating, and updating security protocols, as well as learning to anticipate such critical situations quickly and effectively by testing alternative topologies, and so on, minimizing handling costs and life losses.

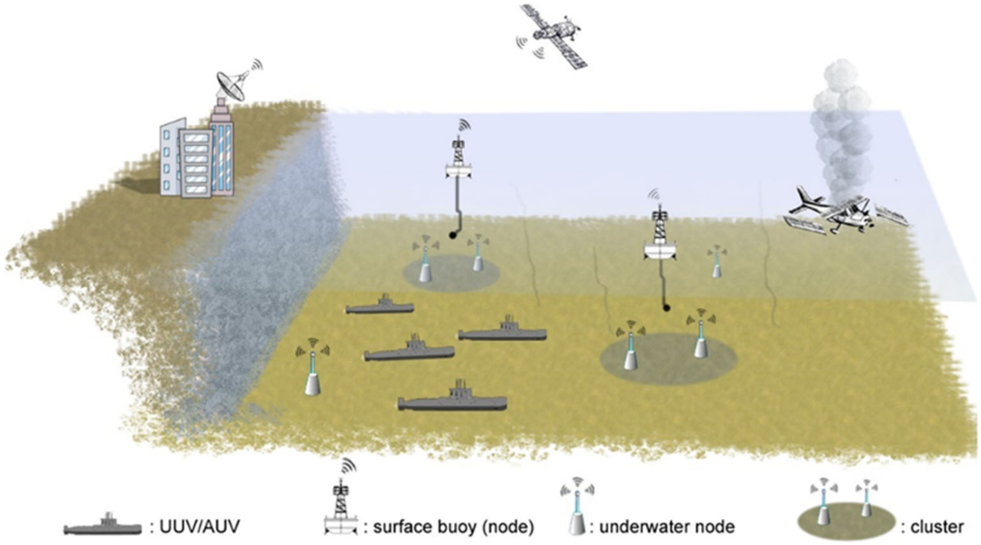

Figure 1. Physical topology of a SAR scenario involving UUVs and other IoUT assets interoperating.

Based on our experience, it must be stated that we do not consider SAR scenarios to be different from other IoUT scenarios (e.g., military ones) in terms of cybersecurity. In the era of long-lasting 'cold wars' between numerous nations, SAR operations, for instance, are targeted by the provocative ones as an opportunity to show off power.

The aim of this research is the study of related works, open issues, and challenges, towards the proposal of a novel simulation tool-supported approach to support commanders of military/search-and-rescue operations to effectively make critical and life-saving decisions. More specifically, this paper aims to support SAR and combat commanders with an efficient UUVs swarm simulation environment that will emphasize interoperability and cybersecurity issues, to achieve and establish secure exchange of data/information. Based on this goal the contribution of this paper is two-fold: (a) to review existing methods and tools of semantic modeling and simulation for cybersecurity and interoperability on the IoUT, (b) to highlight open issues and challenges, towards developing a novel simulation approach to effectively support critical and life-saving decision-making of commanders of military and search-and-rescue operations.

The structure of this paper is as follows: Section 2 briefly describes the basic concepts related to the problem and the IoUT domain. Section 3 presents the survey methodology. Section 4 presents the state-of-the-art in related technologies. Section 5 discusses open issues and research challenges. Finally, Section 6 concludes the paper.

2. Background

2.1. UUVs and Swarms

UUVs are decision-making mechatronic systems, which could expand people's underwater activities in the marine engineering construction, underwater search-and-rescue, or ocean ranch operations [5]. They are powerful assets that can operate in underwater missions and operations autonomously and are capable of situation and environment awareness, making their own autonomous decisions, and planning their own trajectories. Moreover, they interoperate with other underwater, surface, and air vehicles or platforms. A UUV can be considered as a knowledge-based autonomous agent [6]. Furthermore, it has the ability of self-management, i.e., self-configuration, self-healing, self-optimization, and self-protection. An interesting, related work reporting on enhancing self-diagnosis and self-adaptation of UUVs, through a "metacontrol" framework with the implementation of ontological reasoning, has been recently published [6]. In the work of UX-1 in the UNEXMIN project (a robot developed to survey flooded old mine sites) [7], the authors were motivated by the lack of real-time communication, proposing a framework to enhance its ability for self-diagnosis and self-adaptation. To interconnect these valuable assets and achieve an efficient exchange of information, localization is mandatory. This capability allows a vehicle to determine its position and orientation in the world, both underwater and at the surface.

Localization ability of UUVs and underwater assets, is more than meaningful in creating vigorous network architectures, due to the facilitation of information sharing. However, this need generates new challenges to overcome. As we have seen in related work [8], there are different localization algorithms that can be applied to a UWSN and are divided in two broad categories, i.e., range-based and range-free schemes. The first category is based on accurate distance and angle measurements, by using different variables such as Time of Arrival (ToA), Angle of Arrival (AoA), etc. While this method is very precise in estimating an asset's position, it relies on strict time synchronization for the exact information transmission and receiving instances. The second one does not use range or bearing information, relying on simplicity, but enhancing the localization error of nodes; this schema is useful for terrestrial sensor networks.

The technological progress of UUVs is required, towards an efficient operation in the marine environment. They are used to mitigate the risk to human lives and decrease the cost of operations. The need for smart and durable UUVs increases as the maritime operations become more complex and riskier, for instance, supporting the installation of oil and gas facilities or settling underwater cables in depths that were previously unexplored. In addition, in the context of military operations in an IoUT environment, a team of UUVs, each having an individual role and being interconnected, is participating in search-and-rescue operations (SAR) or in mine deactivation operations in Anti-Submarine Warfare [9,10]. Moreover, the interoperability of the UUVs is an issue of consideration when planning an operation, especially when they operate in a swarm formation. A swarm system of independent assets is a group of self-organizing autonomous agents aiming at the effective accomplishment of various collaborative tasks [11].

2.2. Swarm Simulation

In IoUT, the safe and secure movement of an underwater vehicle is a key issue. Especially in a swarm of UUVs, where efficient cooperation between agents is a challenging goal, the difficulties that emerge are tremendous, such as the secure movement and interoperability, as well as the secure communications between them. It is well known that science often tries to copy nature, thus, from the observation of flocks of birds, UUV/UAV technology has been developed [12]. The limitations and constraints of moving from nature to science are many, nevertheless significant advancements towards the development of autonomous UUVs operating in a swarm have been already accomplished. The Science Department of the Universita degli Studi Roma Tre proposed a new type of autonomous underwater vehicles (AUVs) swarm and simulated its operation in a diffused environment.

They have developed an AUV with specific characteristics, without emphasis on robustness, with auxiliary systems such as a camera for taking pictures and classifying fishes or recognizing contamination. They have simulated a swarm of 25 AUVs, studying their movement, interconnection, and performance of their systems, using Matlab/Simulink tool [12]. Having neither a central platform to send further instructions for the operation nor a "leader" vehicle, the results obtained were satisfactory. The Naval University of Engineering in China, similarly using Matlab, a dataset from GEBCO (General Bathymetric Chart of the Oceans) for coordination, a grid system, and a fusion algorithm based on PSO (particle swarm optimization) and ACO (ant colony optimization) named PACO, proposed an approach for autonomous UAV path planning, verifying the effectiveness of their approach [13].

2.3. Internet of Underwater Things (IoUT)

Nowadays, technological innovations allow millions of devices to connect to the global network. This industrial revolution was described by the term IoT (Internet of Things) and was led by the need of users to be constantly connected to their devices to conduct daily activities [14]. The IoT supports a 'smarter' way of living, assisting daily tasks and our wellbeing, such as home automation. Regarding the underwater (sea) "world", there were various daily tasks which could be facilitated, and numerous devices of underwater vehicles needed to interoperate in an underwater sensor network (UWSN) or underwater wireless communication network (UWCN) [15]. Sea species tracking, maritime security and naval military activities and gas/oil extraction are some of these activities. The Internet of Underwater Things (IoUT) has been introduced, not necessarily to simplify such tasks, but to support the efficient interconnection of underwater vehicles, devices, and sensors to the Cloud. The IoUT has brought new research and development directions in a new ecosystem which facilitates the connection of assets "living" underwater and on the sea surface. It aims to tackle several challenges of UUVs such as interoperability, data management, and secure communications, contributing to the development of research, business and underwater military or civil operations [15]. In such an ecosystem, there is a need to establish a fault tolerance connection between underwater and surface assets, meeting key requirements such as heterogeneity, network coverage, low latency, low power usage or battery efficiency, and cyberattacks. The IoUT must integrate heterogeneous assets, to be able to interoperate effectively in UWCNs and UWSNs. Specifically, a UWSN has its own requirements (longevity, accessibility, complexity, security, and environmental sustainability), and the need for a taxonomy based on specific key attributes, such as architectural elements, communication, routing protocol, security, and applications [16]. The establishment of a robust and secure underwater ecosystem is a continuous process as the threats to be countered are becoming more and more sophisticated.

IoUT has certain similarities to IoT such as its structure, function, and its energy limitation. However, a few differences exist, which are related mainly to the heterogeneity of assets in terms of their: (a) communication technologies, (b) tracking technologies, (c) low battery capacity and difficulty of recharge, (d) energy harvesting technologies, (e) network density, (f) localization techniques [17]. Therefore, as mentioned in [18], in order to successfully establish a UWCN/UWSN, and obtain IoUT capabilities, at least the following issues must be considered: (a) the communication medium, i.e., the water, (b) the dynamic changes of network topology, (c) the energy consumption and maintenance constraints, (d) the hazardous environment and physical security, and (e) localization [18].

Limited bandwidth, transmission media (acoustic communication) and low propagation speed of IoUT, in combination with the volume of data to be transmitted, as in IoT, lead to delays in information distribution. This fact allows cyber-adversaries to remain further undetected and achieve their goal efficiently. More specifically, slow transmission rates has consequences of the delayed evaluation of an alert and the delayed reaction to a cyberattack. A way to deal with limited bandwidth and delay in underwater communications and environmental and ambient noise [19] on a communications channel, is the development of data analysis software to optimize the process. Such a method is proposed in [20], to balance data traffic loading in an underwater network and minimize latency issues. This is conducted by presenting intelligent data analytics (IDA), which support high packet allocation in combination with low latency and less energy consumption. Another way to support data gathering and overcome bit-rate issues is the creation of distinct communication channels in underwater sensor networks, such as UWSN [16]. Similarly, implementing an information-centric model facilitates the solution to this challenge. Therefore, in [21] a depth-based caching mechanism is recommended, in order to balance latency issues and exchange of unnecessary information, indicating that the creation of hybrid communication models is very important to overcome the physical phenomena of the water and further develop IoUT.

Fifth generation (5G) and the upcoming sixth generation (6G) connectivity networks are making essential improvements already to the interconnection of IoUT assets, facilitating their communication and exchange of data with tremendous speeds (>1 Gbps) on a large number of devices. In related work [15], the optical wireless communication (OWC) is proposed with the aim to improve underwater wireless communication, concluding that OWC with RF technology can solve big issues in the underwater domain, such as the efficient management of big data, with high bandwidth, low latency, high protection, and low fuel usage.

2.4. Semantic Modeling in IoUT

Semantic modeling concerns the conceptual modeling of domain knowledge in order to describe structured data (with formal semantics/metadata) in a specific logical way. Ontologies are formal vocabularies of concepts and relations, used for the semantic modeling and integration of heterogeneous data. An ontology is defined as the formal and explicit specification of conceptualizations which are used to assist programs and humans to share knowledge, describing entities and relationships among them [22]. Ontologies are versatile tools that provide the means for machines to understand the meaning of terms provided in natural language. They should be reusable in terms of their concepts, axioms, instances, and relationships. Furthermore, according to the NeOn (networked ontologies) [23] methodology, ontologies should offer interoperability, modularity, and extensibility. Formal ontology employs machine-readable languages such as the Resource Description Framework Schema or the Web Ontology Language (RDFS/OWL), in combination with other semantic tools such as query engines, knowledge management tools, and automated reasoners. Semantic reasoning is the ability of a machine to infer logical consequences from a set of asserted facts [24]. Ontologies can improve the interoperability of IoUT assets.

A hybrid approach of context reasoning for underwater robots is proposed in [25], to cover the uncertainties of underwater environments. With the aim to expand the collaboration and cooperation of UUVs/AUVs, as well as the context-awareness concept, an ontological, rule-based, and Multi-Entity Bayesian Network (MEBN) reasoning method is proposed. This framework is proposed to support the SWARM project and SWARM ontology [26], presenting a complete approach to context management and modeling of heterogeneous contexts using ontologies for underwater robots. Information fusion and reasoning techniques improve standardization, and provide a joint scheme of understandable information exchange, supporting cyber and trajectory situational awareness. Situational awareness (SA), which is a necessary condition for UUVs to be able to interoperate and to move safely, is represented in the ontology [27]. To achieve an autonomous decision-making loop for the “leader” of a swarm, it is critical that data can be handled effectively across various platforms and domains, and should be able to be reviewed, stored, accessed and shared efficiently. Almost as important as the mission and path planning is the adaptability of the mission and the recovery from failures [28]. The issue emerges when different protocols of communication are used, and due to the lack of standardization, interoperability is much more difficult to achieve. Semantic modeling of common communication protocols represented as ontologies is required to accomplish semantic interoperability between IoUT assets. It enables autonomous vehicles to understand the environmental situation, integrate new technologies by identifying them almost dynamically, perceive the reason of its actions and the purpose of its existence, and create the desirable autonomous decision-making loop.

2.5. Interoperability in IoUT

The Institute of Electrical and Electronics Engineers (IEEE) defines interoperability as "the ability of two or more systems or components to exchange information and use the information exchanged" [29]. As depicted in Figure 2, interoperability expands in six layers, based on the capability of interoperation between systems [30,31]. Although, in our review we will focus on the first three layers, namely technical, syntactic, and semantic, in which network/connectivity and simulation/implementation are achieved. In UWSNs, where interoperability is inextricably linked to communication and achieved by the transmission of acoustic and electromagnetic signals, water as a medium is an important deterrent. With the aim to overcome the principal issue of IoUT, i.e., interoperability, the authors in [32] propose the SUNRISE model, which implements an abstraction layer for supporting the interconnection of various control software of different underwater vehicles. Motivated by the first initiative to define a common language, which is JANUS from NATO Science and Technology Organization—Centre for Maritime Research and Experimentation (STO CMRE) [9,10], and its being limited to initial contact and emergency message exchange, the authors created possibilities for a heterogeneous network of mobile assets. Encoding and decoding of messages is mandatory, even if a common physical coding scheme exists; any interaction between underwater assets using different control software isn't possible. Therefore, a protocol named SSC (Software-to-Software) is proposed, supporting the cooperation of heterogeneous platforms, e.g., MOOS (https://oceanai.mit.edu/moos-ivp/pmwiki/pmwiki.php?n=Main.HomePage, accessed on 20 November 2022), ROS (https://www.ros.org/, accessed on 20 November 2022), DUNE (https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2350792?locale-attribute=en, accessed on 20 November 2022), etc. SSC provides simplicity, ease of implementation, extendibility, and expressiveness. However, the automated integration of an autonomous vehicle in a network of a swarm of UUVs/AUVs remains a challenging goal.

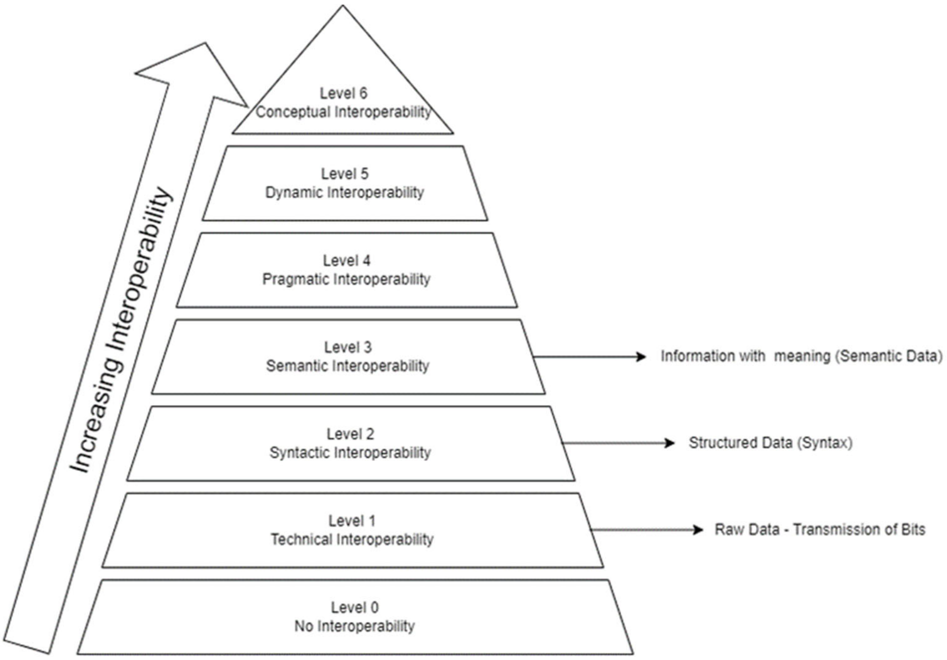
Increasing Interoperability
Level 6
Conceptual Interoperability
Level 5
Dynamic Interoperability
Level 4
Pragmatic Interoperability
Level 3
Semantic Interoperability
Information with meaning (Semantic Data)
Level 2
Syntactic Interoperability
Structured Data (Syntax)
Level 1
Technical Interoperability
Raw Data - Transmission of Bits
Level 0
No Interoperability

Figure 2. Levels of Interoperability.

2.5.1. Technical Interoperability

The principal obstacle in achieving a robust interoperability is the seamless interaction between devices and people with devices [33]. Technical interoperability is probably the most demanding among the three levels, mainly due to the lack of standardization in communication protocols [34]. It is divided into three types: interoperability of devices, networks, and platform as follows.

- Device Interoperability

This concerns the need to add a new sensor or device in an existing network (USWN), with its own communication protocol and power consumption architecture, interoperating with existing devices of the network [31]. The key issue at this level is the heterogeneity of platforms of institutions or the NATO standards. NATO identified the need to further investigate the key issue of interoperability, the standardization, and the lack of common communication protocols. A representative approach for tackling this issue is the initiative to define a common language to achieve initial contact and data exchange between nodes, namely, the JANUS at NATO STO Centre for Maritime Research and Experimentation (CMRE) [9,10,35–37]. This is the first underwater digital communications protocol which was promulgated as a NATO Standardization Agreement (STANAG), enabling interoperability between heterogeneous military and civilian devices.

- Network Interoperability

This concerns the communication protocols used to meet the requirements of a device to interoperate within a network. The key issues at this level are the quality of service (QoS), scalability, fault tolerance, and security of the network. To ensure robust underwater communication networks, an initial discovery protocol is required and, as mentioned above, JANUS is such a protocol. Essentially, JANUS provides all the requirements in order for all assets of the underwater domain to be able to communicate each other in a standard and common language [38].

- Platform Interoperability

Different data sharing policy and operating systems in each platform, such as Microsoft Azure Cloud or Apple Home Kit, result in heterogeneous systems that increase the problem of interoperability [31]. Referring to IoUT, UUVs should be capable of exchanging information efficiently with other underwater platforms, but also with surface and air platforms. Some of the most important data or messages needing to be exchanged, among others, are related to the a) coordination of friendly units or enemy targets, b) their trajectory information, (speed, course, depth), c) their classification in recognized types, d) fuel and battery residues, and e) ammunition residues. An effort to achieve effective exchange of such data between heterogeneous platforms has been proposed by researchers from the Applied Research Laboratory at the University of Hawaii (ARL at UH), the RIP Laboratory at the University of Hawaii at Manoa, the Naval Undersea Warfare Center Division Newport (NUWCDIVNPT), and the Underwater Systems and Technology Laboratory at the University of Porto (LSTS) [39]. Numerous unmanned platforms, including USVs, and UUVs, utilized different open-source software stacks in order to interoperate and “speak” the same language. Moreover, an underwater node had the task to continuously order new higher-priority plan-paths to the UUV. Several challenges were encountered, with the most significant being the integration of different communication protocols of platforms, concluding that integrating the new JANUS standard is probably a solution for most of the challenges in interoperability in the underwater domain.

2.5.2. Syntactic Interoperability

Syntactic interoperability concerns the interoperability of data formats (e.g., csv, json, xml, rdf) when transmitting or receiving data or information or services between heterogeneous devices, sensors, and systems. The aim is to provide an approach able to encode and decode data sent from and received by everyone.

2.5.3. Semantic Interoperability

Semantic interoperability concerns the ability of computer systems and applications to exchange data unambiguously, i.e., under a common and shared understanding of the context and the domain of discourse [40]. A global shared and commonly agreed ontology followed by the common interpretation of semantic information, would be the ideal case [41]. However, the lack of standardization, and the extension of ontology when reusing it, makes the issue of data exchanging with shared meaning constantly bigger. Semantic interoperability provides the ability to enable machine-computable logic, and (therefore) the skill of exchanging meaning with data (i.e., data semantics), in combination with the packaging of data (data syntax). It is a recommended solution to interconnect all devices in an IoUT environment, but also to integrate the human factor. For example, considering that in a swarm of UUVs, various types of vehicles exist (e.g., attacking, surveillance and cyber-surveillance), thus different capabilities, this results in the need to integrate a variety of their heterogeneous sensors and systems. Consequently, in an underwater network, a torpedo firing system, a surveillance radar, and a radar of a UAV that coordinates a target, should all be able to exchange information between each other in a common language. NATO aims to provide solutions to a wide range of underlying problems in interoperability of heterogeneous platforms [10], in processing and interpretation of increased volumes of sensor data, including military command and control (C2) systems, in combination with low-power and long-endurance operations, by experimentation and standardization of protocols (STANAGs). More specifically, the CMRE Data Knowledge and Operational Effectiveness (DKOE) team developed the Fusion and Reasoning under Uncertainty Modelling (FORUM) research platform, developing an ontology for describing experimental evaluations for the recognition of different classes of ships [10].

Although UUVs constantly gain popularity, the problem of interoperability between heterogeneous platforms for a multi-vehicle, multi-domain missions are still open [39]. It is crucial to work on a cross-domain communication and interoperable protocol, in order to connect platforms of different manufacturers, architectures and interfaces, similar to the work conducted on JANUS in CMRE. The road towards overcoming issues of interoperability of UUVs is challenging. It is essential to exchange information such as geographical position or trajectory elements between surface and/or air platforms, as well as to ensure the integrity of the information and to avoid packet loss, considering the restriction of low energy consumption. Furthermore, the robustness of an underwater network is important to guarantee the availability of data. Motivated by this necessity, a routing protocol is presented, named Efficient Void Aware (EVA), to detect the void nodes and suppress them from the eligibility to forward data packet [42]. The general idea is similar to the "ping" command used to check connectivity between two end devices over a network. According to the proposed protocol, before every transmission of information from a UUV to a heterogeneous platform and vice versa, a "test" packet is being sent to evaluate the availability of other devices. Although the proposed idea is ostensibly effective, many security and bit-rate issues are emerging due to the increase level of the packet transmissions, which results in network congestion. Nevertheless, there is a long way until a framework can connect all these heterogeneous sensors and systems, being able to manage heterogeneous data in such a way that all the platforms communicate under a commonly understandable language.

2.6. Cybersecurity in IoUT

Nowadays, the term "communication" is implicitly linked to security. The technological advancements that are taking place every day in numerous domains, such as industrial IoT, digital twins, 3D printing, quantum computing, security blockchain, etc., have exponential growth. Upcoming trends such as 5G, IoT connectivity, Cloud computing, etc., are becoming part of our daily life. However, the major issue of this rapid technological development is the difficulty, in most cases, to follow along [43]. The tremendous development of information and communication technologies (ICTs) and automation of most processes in our daily life, improve mobility by offering a variety of services to a vast number of users [44]. However, vulnerabilities are raised even more, impacting users directly from the security perspective. The principal issue concerns non-awareness of the power of constantly emerging trends and the fact that users cannot perceive their function. Undoubtedly, the weakest link in defense against cyberattacks is the human being [45]. Internet of Things (IoT) in combination with 5G can connect huge number of devices with huge speeds, but the majority are not aware of the potential threats this facilitation seeks. This increases the number of potential access points for cybercriminals [46], and a great example is the era of COVID-19, in which remote work constantly raised extreme risks. From free-access hotspots to personal devices, adversaries can find a path to exploit them and extract our personal data; in fact, according to the UK National Cyber Security Centre, in the first quarter of 2021, there were three times as many ransomware attacks as in the whole of 2019 [46].

Numerous security issues and vulnerabilities are emerging regularly, in networks across all domains. Unfamiliarity with technology, is one of numerous and various reasons security systems fail to detect and defend against sophisticated attacks. Statistics from IBM's Cost of a Data Breach Report 2021 [47] indicate that the average cost of a data breach increased by 1.07 million USD in 2021. Furthermore, according to ENISA's (European Network and Information Security Agency) Threat Landscape 2021 [48], DDoS attacks, a denial-of-service attack that malfunctions a network, have shown an upward tendency the last two years. Additionally, an infamous (in the cybersecurity community) virus named Emotet botnet, one of the longest-running and most widespread malware threats which is spread through spam emails, dealt a major blow, due to its enormous impact, especially in Windows administration and control servers [47]. Adversaries from "script kiddies" to the experienced can perform devastating attacks; most of these attacks concern networks and communication protocols between the host and the server. However, innovative tools can utilize new technologies to counter cybercrime. AI-powered cybersecurity for example, can predict vulnerabilities and identify suspect patterns, to alert incident responders for possible attacks. Thus, an interesting project, known as AIDA [49], utilizes artificial intelligence (AI) combined with machine learning (ML), in order to establish effective data analytics. Consequently, by developing big data analysis and an analytics framework equipped with automated data mining to deal with information extraction and knowledge management, they contribute to counter cybercrime. The project is expected to be completed by the third quarter of 2022. Vulnerabilities and cyber threats exist across all domains, and it is undoubtedly irrational to deny their existence as well in the domain of IoUT. To ensure the security of the underwater domain, robust security systems equipped with effective frameworks and semantic knowledge are a recommended solution, offering suitable methods for "uncharted" behavior; the main issue of the cybersecurity domain [50].

Attack methodologies and tools are becoming more and more sophisticated, generating the need for determination of the specific steps of an attack. Cyberattacks are divided in two broad categories: (a) active and (b) passive. The typical cycle of a cyberattack has the following order: (a) reconnaissance (physical/social and Web/host), (b) scanning and enumeration, (c) gaining access (exploitation), (d) maintaining access, and (e) covering tracks. As a cyberattack defender or cyberattack analyst, the first two steps are the most crucial to prevent an attacker from enumerating and exploiting a network. Furthermore, accuracy in data recording and their analysis, have become challenging goals, mainly due to the data visibility challenges, which concerns the degree of ease by which data can be monitored and analyzed from numerous sources. It is very important to mention that almost every security mechanism an enterprise employs affects data visibility negatively. For example, the use of HTTPS (Hypertext Transfer Protocol Secure) protocol, which provides end-to-end secure connectivity, does not allow a security analyst to monitor data traffic. Nevertheless, several standards have been developed to tackle this issue, such as chain of custody (ISO standard 22095, https://www.iso.org/standard/72532.html, accessed on 20 November 2022), concerns "the chronological documentation that records the sequence of custody, control, transfer, analysis and disposition of materials, including physical or electronic evidence", supporting the traceability of data.

The use of digital systems is now essential for civil/military maritime activity. This digitalization to help the automation of tasks without human interaction, in combination with the cooperation of a swarm of underwater assets, increases complexity in early detection of attacks, results in various weaknesses [51] and raises vulnerabilities in an exponential manner. Furthermore, security assurance, which is defined as: "the degree of confidence that the security requirements of an IT system are satisfied" [52] is not ensured. Threat assessment, risk analysis and modeling techniques enable IT systems to map security, privacy, and safety requirements, to specific counter measures [52]. Numerous standardized methods for industrial cyber risk assessment exist, with the most remarkable being the Formal Safety Assessment (FSA) and Cyber Preliminary Hazard Analysis (CPHA). The first one concerns "a structured and systematic methodology, aimed at enhancing maritime safety including protection of life, health, the marine environment and property, by using risk analysis and cost-benefit assessment" [53]. On the other hand, CPHA [54] requires several steps to establish a Security Risk Assessment and document all possible hazardous scenarios [54].

It is a fact, that most of the attacks carried out on the surface are undoubtedly achieved in the underwater domain also. In IoUT, which incorporates various special characteristics, the risk of a cyberattack or exposure of sensitive information is increased, and the attack surface is expanded, namely the aggregation of vulnerabilities of a system. Due to the dynamic environment of IoUT, where uncertainty, heterogeneity, and big data generate potential vulnerabilities, there is an extremely high demand to establish real-time cybersecurity assessment. Moreover, slow bit-rate issues make the rapid alert evaluation unfeasible. Numerous methods are appropriate in achieving confidentiality, integrity, and availability in underwater communications, nevertheless, the priority should be the consolidation of security requirements considering the various components of this domain, the diversity of communication protocols and physical phenomena of water. Several cybersecurity frameworks have been developed to support and automate the process of protection from cyber adversaries and reduce cybersecurity risk. This process usually comprises standard steps such as detect, respond and recover. An example of the implementation of such a framework (National Institute of Standards and Technology—NIST framework, https://www.nist.gov/cyberframework, accessed on 20 November 2022) in UUVs' functions is depicted in Figure 3.

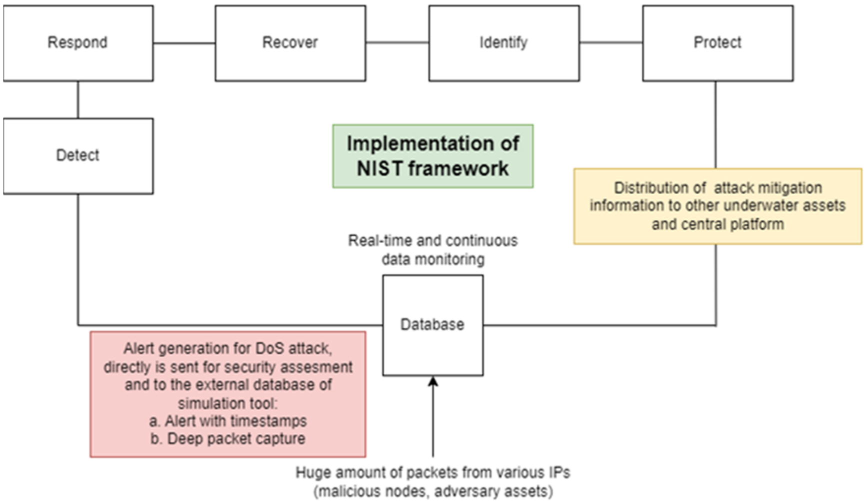
Respond
Recover
Identify
Protect
Detect
Implementation of NIST framework
Distribution of attack mitigation information to other underwater assets and central platform
Real-time and continuous data monitoring
Database
Alert generation for DoS attack, directly is sent for security assesment and to the external database of simulation tool:
a. Alert with timestamps
b. Deep packet capture
Huge amount of packets from various IPs (malicious nodes, adversary assets)

Figure 3. Implementation of NIST cybersecurity framework during a DoS attack.

Typically, the sequence is attack–defense–attack, and the attacker is ahead of security and intrusion detection systems (IDS). The most remarkable security challenges in IoUT are (a) node compromise, (b) routing attacks, (c) denial of service attacks [18]. However, network sniffing [55], a method of reconnaissance which is described as capturing passively information about a network environment, is the origin of every disastrous cyberattack. Being impactful especially for military operations due to the high need of confidentiality for sensitive information, this method is achieved by eavesdropping (sniffing) traffic of packets, when transmitting data over a wired or wireless network. Subsequently, regarding the underwater domain, adversaries can potentially reveal critical information about the location of an underwater asset or a surface platform. A devastating attack, which can be executed despite the presence of protection mechanisms, such as multi-factor authentication and strong encryption algorithms [18], is the denial of service (DoS) Attack and distributed denial of service (DDoS) attack; a network layer (Layer 3 of the OSI—Open Systems Interconnection model) attack, but also in the application layer (Layer 7 of the OSI model). The attacker floods the network with huge amounts of queries, forcing devices to consume resources, preventing regular traffic from reaching its destination. In a complex and hazardous environment such as the IoUT, in which interoperability between heterogeneous assets is critical, a DoS attack could cause tremendous results. Consequently, a swarm of UUVs would be unable to receive information from the central platform or redistribute proper information to the rest of the units, affecting their adaptive decision-making and path-planning capabilities. Moreover, in [56], a very common and effective physical layer attack, known as jamming, is described in detail. The aim of this attack is the disruption of communication channels between hosts, in underwater domain nodes, or between other underwater assets. Additionally, due to dependence from the energy factor in IoUT, jammers are becoming even more dangerous. Their ability to reduce the lifetime of nodes by forcing them to unnecessarily transmit packets of traffic continuously, causing congestion and latency, allow attackers to achieve their goal efficiently. By simulating jamming in a realistic channel and considering that the jammer has a limited lifetime and the same characteristics as a friendly node, we conclude that this attack is nearly always successful.

3. Research Methodology

This section describes the research methodology followed in this paper, which focuses mainly on the collection of information sources related to existing research gaps of the semantic modeling and simulation of cybersecurity and interoperability on the IoUT, as well as the formalization of information to be extracted. The research was conducted in a period of six months, examining academic articles, relevant literature and Web resources published between 2016 and 2022 (6 years) and it was accomplished in four steps, as depicted in Figure 4: (a) research design, (b) research conduction, (c) experimentation with tools, (d) conclusions.

Regarding the research on simulation methods, the focus was on methods that facilitate the prediction of outcome of an operation before it happens, by entering data in a simulation/prediction software. Additionally, new trends in simulation technology, i.e., digital twins, were included. In order to extract detailed information through current literature regarding the abovementioned concerns, we employed the PRISMA methodology.

Therefore, we formed two primary and one secondary research questions as follows.

Primary questions:

1. What are the current semantic modeling and simulation approaches regarding interoperability in the IoUT? (Figure 5).
2. What are the current semantic modeling and simulation approaches regarding cybersecurity in the IoUT? (Figure 6).

Secondary question:

3. How can related research problems be overcome using new technologies, such as the technology of digital twins?

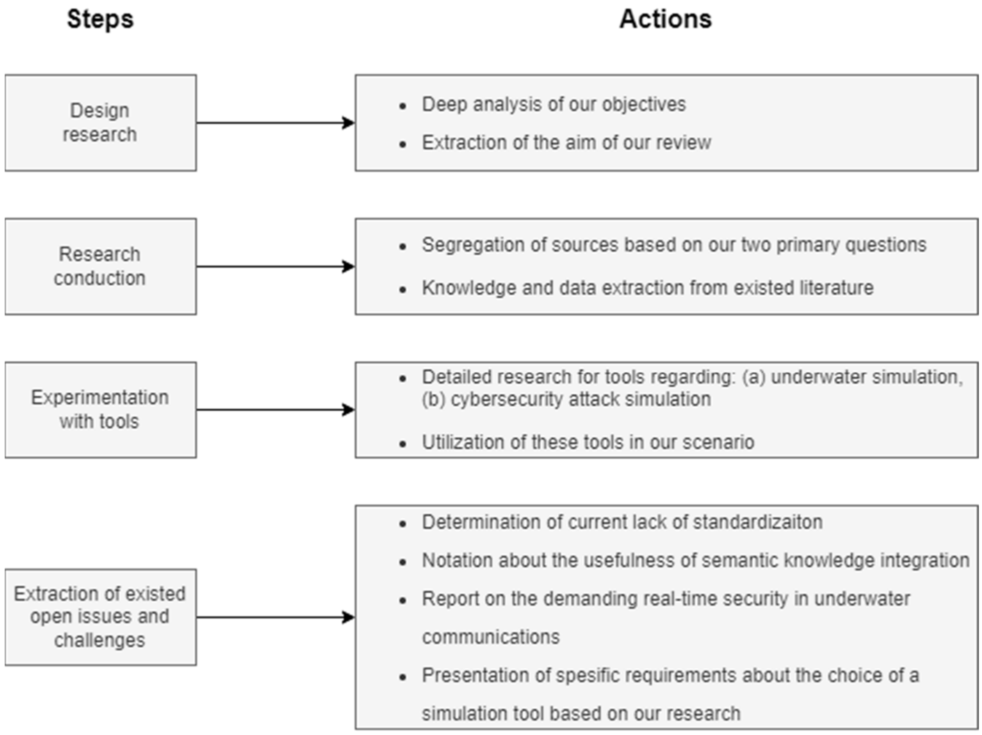
Steps
Actions
Design research
Deep analysis of our objectives
Extraction of the aim of our review
Research conduction
Segregation of sources based on our two primary questions
Knowledge and data extraction from existed literature
Experimentation with tools
Detailed research for tools regarding: (a) underwater simulation, (b) cybersecurity attack simulation
Utilization of these tools in our scenario
Extraction of existed open issues and challenges
Determination of current lack of standardizaiton
Notation about the usefulness of semantic knowledge integration
Report on the demanding real-time security in underwater communications
Presentation of spesific requirements about the choice of a simulation tool based on our research

Figure 4. Steps of conducted research.

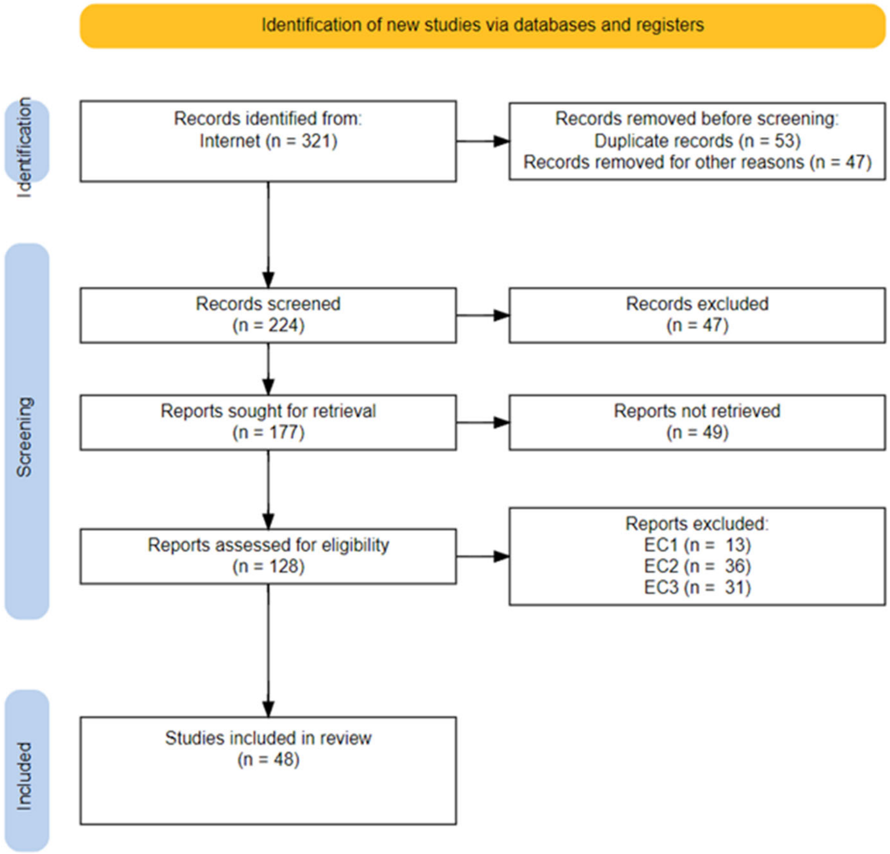
Identification of new studies via databases and registers
Identification
Screening
Included
Records identified from: Internet (n = 321)
Records removed before screening: Duplicate records (n = 53) Records removed for other reasons (n = 47)
Records screened (n = 224)
Records excluded (n = 47)
Reports sought for retrieval (n = 177)
Reports not retrieved (n = 49)
Reports assessed for eligibility (n = 128)
Reports excluded: EC1 (n = 13) EC2 (n = 36) EC3 (n = 31)
Studies included in review (n = 48)

Figure 5. PRISMA flowchart of first primary question.

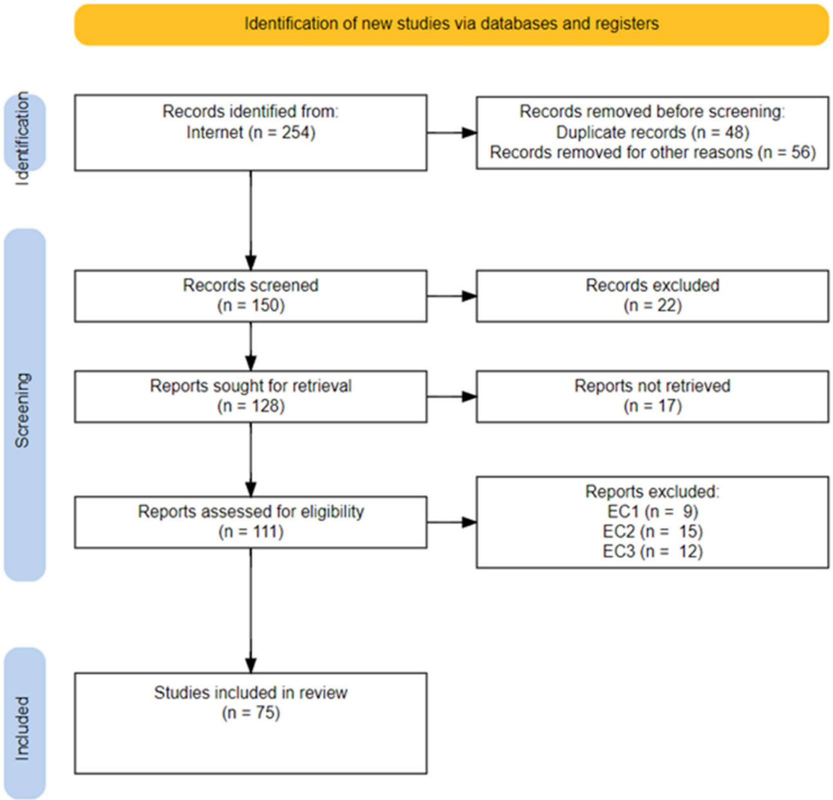
Identification of new studies via databases and registers
Identification
Records identified from:
Internet (n = 254)
Records removed before screening:
Duplicate records (n = 48)
Records removed for other reasons (n = 56)
Screening
Records screened
(n = 150)
Records excluded
(n = 22)
Reports sought for retrieval
(n = 128)
Reports not retrieved
(n = 17)
Reports assessed for eligibility
(n = 111)
Reports excluded:
EC1 (n = 9)
EC2 (n = 15)
EC3 (n = 12)
Included
Studies included in review
(n = 75)

Figure 6. PRISMA flowchart of second primary question.

With the aim to present existing methods and tools of semantic modeling and simulation for cybersecurity and interoperability on IoUT, a detailed review through existing literature has been conducted on general search engines (Google/Bing) and on academic Web portals such as Scopus, Google/Semantic Scholar, and ResearchGate. The specific search terms (keywords) used in combinations were:

- internet of underwater things
- semantic modeling
- ontology
- open source
- simulation tools
- underwater network
- underwater environment and communication
- wireless communication
- unmanned underwater vehicle
- autonomous underwater vehicle
- swarm
- interoperability
- cybersecurity
- cyber threats
- risk assessment
- threat and vulnerability modeling
- search-and-rescue operation
- communication standardization
- digital twins

Selection/rejection of literature was carried out based on specific inclusion/exclusion criteria, in order to filter yielded results from above questions, and to extract the most relevant data.

- **Inclusion Criteria**

  IC1. Articles presenting simulation approaches with desired and undesired results.
  IC2. Articles related to each research question separately.
  IC3. Articles related to interoperability and cybersecurity in IoUT.
  IC4. Articles related to the abovementioned specific keywords.

- **Exclusion Criteria**

  EC1. Articles written in non-English language.
  EC2. Articles published before 2016.
  EC3. Articles referring to cybersecurity methods that cannot be applied in IoUT.

Moreover, to provide solely open-source, non-obsolete and with specific requirements simulation tools, we employed several sub-criteria, as described in [57,58]. Table 1 provide an overview of these general sub-criteria, distinct for underwater and cybersecurity domains.

Table 1. Sub-criteria for selection/rejection of network simulation tools.

Sub-Criteria	Explanation
Accessibility	Availability of source code on GitHub
Up-to-date and version	• Non-obsolete tools • Commitment on GitHub two (2) years ago maximum
Programming language	The main programming language the simulation tool is written (focused on Python, due to the extensive library availability)
Testing and efficiency	Whether the software developed for underwater environment or cyberattack for underwater environment
Input	• Format of data it accepts (e.g., .xml, .rdf, .ttl, .owl, etc.) • Interaction with data (if it accepts dynamic data from a database and live applications)
Output	Whether it can represent knowledge in a visualized environment or extracts statistical data, analytic reports, graph models, etc.
Integrity	Integration with other software packages
Execution	• Whether it can run discrete simulation or multiple instances at a time • Whether user can specify values initially or during the simulation process
Limitations	Size of the input data it accepts, number of nodes, accuracy of time data, etc.
Documentation	Availability of manual, recent literature, and helpful videos

In addition, due to the broad domain of cybersecurity, Table 2 provides several additional criteria for the selection/rejection of simulation tools regarding this domain.

Table 2. Additional criteria for selection/rejection of cybersecurity simulation tools.

Sub-Criteria	Explanation
Attack lifecycle	Whether it can simulate the full lifecycle of an attack (pre-compromise, post-compromise)
Up-to-date libraries	Updated with current sophisticated attacks
Report	• Extraction of conclusions (not raw data for verification from the user) • Real-time reporting, as the simulation runs
Integration	Integration with cybersecurity frameworks for risk and vulnerability assessment
Customization	Whether user is capable of customizing values and elements of an attack
Realism	Whether the scenarios, attacks and defend procedures simulated correspond to realistic incidents

As depicted in Figures 5 and 6, in order to extract information which answers the selected research questions, we gathered numerous and various reviews, regulations, conference papers, reports and online blogs. The obtained results were filtered based on their content by using the above-mentioned keywords. Finally, in this review, the presented knowledge emerges solely from open resources related to the semantic knowledge and cybersecurity topics.

Regarding the second primary question, we identified 254 articles as represented in Figure 6, following the same inclusion and exclusion procedure.

Articles which mainly cover issues related to the interconnection of heterogeneous systems, platforms and sensors, secure underwater communications, safe movement, and simulation methods, were included. In addition, considering the absence of standardization and formalization of required information during a SAR or military operation, articles from this domain were not included. We were relied on personal experiences during our participation in related missions, supporting the uninterrupted and secure exchange of information, and introducing new factors for further research in the domain of IoUT.

As new generation technologies connect a vast number of heterogeneous devices, resulting to numerous cyber threats and vulnerabilities for adversaries, as well as complex architecture of networks, our focus is on how to efficiently research and combine the topic of cybersecurity with the topic of semantic interoperability, in the domain of IoUT. Therefore, we have focused our study on considerably several articles related to cyberattacks and automation processing for their early detection and mitigation by the utilization of semantics and reasoning in underwater wireless sensor and acoustic networks (UWSN/UWAN).

4. Results: State-of-the-Art Approaches

4.1. Semantic Modeling in IoUT

4.1.1. Semantic Modeling and Interoperability

In the work of Migueláñez et al. [59], a framework is proposed for supporting the idea that heterogeneous data should be processed by systems using different protocols, and these data should be finally available and accessible, to be also reviewable, by a higher-level decision-making agent. The proposed method uses a pool of hierarchical ontologies for the representation of the knowledge extracted from the experts (human) and from the processed sensor data. Moreover, this is the first approach to a specific goal-based autonomous planning using a semantic representation approach. Authors implement the concept of situational awareness (SA) of the vehicle, allowing the perception of the big picture by reusing existing ontology. The approach re-engineers the core ontology into a Status Monitor Application Ontology to represent SA, and into a Mission Planning ontology to integrate an adaptive goal-based decision-making process. The proposed framework has been evaluated against the problem of fault-tolerant adaptive mission planning. Based on the combination of two techniques, i.e., ontological representation of knowledge and adaptive mission planning repair techniques, their benefits are highlighted by showing the interlinking and interoperation of the two ontologies within the testing context.

A common information model is the key for cooperation of UUVs. However, uncertainty of events that may occur during an underwater operation is very high and this leads to exchange of information with doubtful meaning between UUVs. In the work of Xin Li et al. [59], the SWARMs ontology is presented, which provides uncertainty reasoning and probability annotation by utilizing ontology constructs defined in the PR-OWL (https://www.pr-owl.org/, accessed on 20 November 2022) ontology. SWARMs separate mission and planning modeling in two levels. The first level, high-level planning, support the ease of its handling, by allowing the user to command different tasks to each vehicle, without the need to specify exact actions. The second level, low-level-planning, regards tasks performed at the vehicle level (generation of waypoint, etc.) and also provides multiple surface and underwater unmanned vehicles, and combines networking and communication domains. By incorporating Protege (OWL ontology) and SWRL rules to express complex rule formations and relations, they experimented in a chemical pollution scenario, in which they estimated the emergency level of the polluted region. SWARM, by including several domain-specific ontologies, confronted mainly the uncertainty of the underwater environment; however, its implementation in heterogeneous devices has not yet been accomplished.

In the work of Hongfei Yao et al. [60], an ontology-based marine environment situation awareness information modelling is proposed. Due to the difficulties of predicting uncertain events (target threat, cyber threat, abnormal thruster, water leakage) that may occur during an underwater operation, a core ontology of UUV is represented, in which uncertain events are triggered based on Semantic Web Rule Language (SWRL) rules and Resource Description Framework (RDF). Moreover, as uncertain factors and uncertain knowledge lead to probabilistic knowledge, a probability expansion of OWL language is required. Thus, UUVs are provided with important data for rapid decision-making when an uncertain event occurs. Nevertheless, since ontology cannot reason about uncertainty, it is transformed into a Bayesian network. Simulation experiments verify the effectiveness and accuracy of the situation awareness reasoning method that combines the ontology and the Bayesian network.

Sugyan Kumar Mishra et al. [61], in order to bridge the gap between heterogeneity and manageability of huge number of sensors, proposed an ontological approach by integrating the concept of large-scale service-oriented architecture (SOA) (LSS). Suitable for dynamic environments such as IoUT, this approach extends the existing SSN (https://www.w3.org/TR/vocab-ssn/, accessed on 20 November 2022) ontology by the concept of a large-service domain. By using new properties, this extension provides the ability to detect available or unavailable devices, but also the geographical coordinates, date, and time of the results. The extracted ontological framework is referred to an IoT service-based environment to efficiently use service composition mechanisms in the large service domain. Being reusable and integration-friendly with other ontologies, this ontology concept is easily implemented in IoUT.

Adaptive planning, a main capability of UUVs, is dependent on a key factor, i.e., weather conditions. Extracting accurate information about weather conditions at the exact location of an operation and distributing these data among underwater assets, facilitate their decision-making. An interesting ontological model to integrate meteorological measurements is presented in [62]. By linking several, mainly sensor-based, ontologies (SOSA, SSN, W3C Time Ontology, etc.), they created a real-time dataset (temperature, wind speed, etc.) in CSV format, containing all the individuals that describe measurements of their own weather station in a farm, to support farmer activities. The transformation of these data to RDF triples and their integration, was achieved by a manuscript Python program. The main issue of this project concerns duplicate values, due to recurring information from different sensors. In IoUT, such a model could be integrated in scattered assets, in order to distribute environmental data to other underwater components. However, this demands a massive number of distinct devices, acting solely as weather forecasters, congesting even more of an underwater network architecture.

A possible solution for the above issue is described in the work of Jiantao Wu et al. [63]. An ontology-based approach for environmental data incorporation is presented, by integrating raw data from a well-known database, which generates a massive amount of climate data in real-time from various sources, such as satellites, ships, buoys, radars, etc., named NOAA (National Oceanic and Atmospheric Administration's National Weather Service, https://www.noaa.gov/information-technology/open-data-dissemination, accessed on 20 November 2022). The proposed ontology, i.e., CA (climate analysis ontology), utilizes a SPARQL server, with the ability to store RDF triples and to perform RDF queries. It also employs NOAA CDO (Climate Data Online, https://www.ncei.noaa.gov/cdo-web/, accessed on 20 November 2022), to populate CA with climate data. To map raw data to RDF triples, an open-source Python program (https://github.com/futaoo/codespaceRepo, accessed on 20 November 2022) was developed, based on the Python package *rdflib* (https://rdflib.readthedocs.io/en/stable/, accessed on 20 November 2022). The experimental results with the ontological data model, data processing, ontology creation, and a query engine, prove the overall efficiency of the CA.

Another work for semantic modeling for interoperability, following a different approach, is the one presented by Rahmati [64]. To prevent the potential pollution of water, they propose an adaptive sampling algorithm. By using a swarm of autonomous underwater vehicles as agents, which interoperate with a surface buoy in a Multi-Agent

Reinforcement Learning (MARL) framework, they accomplish an autonomous decision-making loop, with energy and time efficiency. By using reinforcement learning (RL), they conduct adaptive sampling in two phases, exploration and exploitation, in a standard grid–world map. In an obstacle-free underwater/surface environment they succeeded in obtaining the parameters for water pollution in two different locations and in various depths. The issue emerged when the number of autonomous underwater vehicles was increased above 10, making it difficult to observe their behavior.

Motivated by the need to reach unexplored, unsafe, and hazardous environments in deep waters, the authors of [65] present an adaptive visual information (AVIG) framework for autonomous exploration using AUVs [65], which coordinates the parallel execution of four modules: navigation, data processing, map estimating and planning. Differentiating the basic autonomous behavior of an AUV, by adding two high level modules, one for data processing and another for replanning, they used high resolution images from a bottom-looking stereo camera that used a stereo camera driver node. After applying semantic segmentation using a convolutional neural network (CNN), these images were converted into 3D coordinates. In addition, they developed a strategy for decision-time adaptive replanning; having the AUV in constant motion, neither needing to stop, nor being forced to complete the commanded mission paths, in order to replan. The developed strategy for adaptive replanning based on coordination is simulated into a node network inside of a given target area and outside of obstacle areas. Simulations have been performed using the Turbot AUV.

A very crucial step to achieve secure movement and automate underwater operations of self-driving underwater vehicles is object detection and classification, as well as its avoidance, during their trajectory. This can be done either by predefined objects as obstacles in the database of the vehicle, or by real-time image processing, which is more realistic due to the dynamic environment of IoUT. Nevertheless, in a risky and unexplored environment with low visibility, as with deep-sea waters, object recognition is challenging. In related work [66], motivated by the challenges emerging under realistic underwater conditions when collecting real data from an AUV, a combination of 3D object recognition and semantics is proposed by utilizing the Bayesian estimation. Testing was conducted by a lightweight and very stable AUV (Girona 500) consisting of various sensors and systems such as the Global Positioning System (GPS) and acoustic modem. The aim of this test was to successfully explore an underwater industrial structure made of pipes and valves and label them. After successful results, the review concludes that the combination of semantics and Bayesian estimation improves further the object recognition issue.

Another interesting method related to underwater object detection has been recently proposed [67]. In this work, a sonar simulator identifies the semantic information of a viewed scene, and then realistic sonar images are generated from the simulated images. This method can also work vice-versa, something very useful for exchanging information with a UUV/AUV. The procedure of this operation is relatively simple, using a sonar sensor which consists of a transmitter and a receiver. At first, the receiver measures the time-of-flight from a transmitted beam and its intensity to create the image. Next, the image is simulated by omitting physical phenomena of the medium, the water. Hence, in order to overtake underwater environment challenges such as refraction and reflection, which affect the quality of images, they utilized deep learning. The result was images with lower quality, not so representative of the reality, but containing accurate semantic information about the environment.

4.1.2. Semantic Modeling and Cybersecurity

In a dynamic environment such as IoUT, real-time cybersecurity is mandatory. Updates and patches, and cybersecurity assessment, must be a continuous process; in fact, this process should be placed in the top priority of actions taken by operations and management teams. To achieve an efficient real-time cybersecurity risk assessment of a large network, several factors should be taken into consideration. Interoperability and communication between all assets are both vital to gather data/information from the whole internal architecture. In addition, connectivity with external sources is significant in order to be able to correlate suspicious behaviors and acts [65].

In related work [68], authors aim to provide high availability of services used by information technology (IT) systems and minimize the impacts of security failures, thus, they developed an ontology for threat assessment and risk analysis. Initially, they identified the security requirements of unmanned autonomous systems and then they modeled how adversaries achieve their objectives. The technology utilized was the free open-source ontology engineering tool Protégé, the OWL language, and the well-known open-source vulnerability scanner named OpenVAS (https://www.openvas.org/, accessed on 20 November 2022). After the conceptualization and definition of concepts related to the dependencies between risks, threats, vulnerabilities and information assets, the relevant knowledge is extracted from the obtained XML report, allowing intelligent decisions to be made. The semantic modeling and interoperability between cybersecurity solution systems, such as the Intrusion Detection Systems (IDS), should be achieved to be able to integrate all the related data available, towards automating a continuous real-time risk assessment. Based on such an approach, analyzing system activities and identifying known cyberattack patterns is facilitated.

Another approach to support ontology-based knowledge sharing and address common and known threats, attacks, and vulnerabilities, is proposed by Aviad et al. [69]. Combining semantic technology and standardization of countermeasures, the approach effectively achieves provision of a federation of resources of the cyber security domain and the representation of relationships with other concepts (threats, mitigation techniques, etc.) for two well-known attack cases, i.e., the "SQL Injection"(https://portswigger.net/web-security/sql-injection, accessed on 20 November 2022) and the "Heartbleed"(https://heartbleed.com/, accessed on 20 November 2022). The presented model is designed in such a way that enables the combination of resources that either already exist or are future-anticipated, focusing on the attack patterns and supporting them with vulnerabilities, weaknesses, and other various categorizations. Finally, another important feature provided is reasoning, based on relationships ("exploits by", "detectable by", etc.), which facilitate the understanding of the whole concept of attack, providing indicators of compromise (IOCs) (pieces of data such as log files, that identify potentially malicious activity in a network or system [70]) and supporting the perception of the attack pattern, i.e., which component was tried to be exploited, which was the exploit, etc. Furthermore, correlation with well-known knowledge databases is supported (MITRE, OWASP, and WASC).

Well-managed cybersecurity operations demand rapid and accurate identification of an alert, to be able to counter cyber threats. Moreover, modern information systems are characterized by complexity and integrate a vast number of security metrics, which need to be analyzed. Cybersecurity tools can support the prediction and evaluation of the consequences of a cyber threat, but they should be prepared to examine a huge volume of data. Elena Doynikova et al. [71] propose a semantic model, i.e., Ontology of Security Metrics [72], to support security evaluation of information systems and to facilitate the work of security tools. The main goal of this ontology is to accurately determine the goal of a cyberattack and allow for more efficient responding to attacks in future. It provides four basic classes, i.e., data sources, security information, infrastructure objects and security metrics and is implemented using OWL. Security of Metrics can answer questions by importing raw data and provide an efficient security evaluation. The main issue, from our perspective, is the inability to counter the probabilistic behavior of this domain, especially in our era, in which cyberattacks are becoming more and more sophisticated ("zero-day" attacks, https://www.kaspersky.com/resource-center/definitions/zero-day-exploit, accessed on 20 November 2022).

Another related approach is presented by Syed et al. [73], developing a cybersecurity vulnerability ontology (CVO). Since the prevention of cybersecurity exploits requires the integration of vulnerability information from multiple resources, including social media, they designed an ontology to represent the vulnerability domain; in fact, except from integrating common vulnerability concepts from various known resources, they also represent knowledge related to the well-known social media platform, Twitter. Furthermore, they have designed a confidentiality, integrity, and authentication (CIA) system which uses the CVO to represent cybersecurity alerts. CIA essentially receives all the information from CVO and external or internal resources, to deduce the alerts. Eventually, they have evaluated both the CVO and the CIA system, concluding that the quality of CIA alerts generated depends on the underlying ontology.

The first cybersecurity ontology to support broader and heterogeneous security use cases is the unified cybersecurity ontology (UCO) [74]. Due to its variety of entities, relations, actions, events, intentions and plans, UCO is suitable for reuse and integration, as well as for linking other ontologies in this domain. In their work, the authors present their semantic approach to implement situational awareness to cybersecurity systems; they have reused other known semantic approaches, i.e., CVE [75], CCE [76] and STIX [77] of the same domain to extend the standards and the vocabulary in a single unified ontology. Several classes are included, with the most significant being Means, Consequences, Attack, Attacker, AttackPattern, Exploit, Exploit Target, and Indicator; moreover, there are several classes that refer to the network and architecture of the system, such as Network State and Processes. Additionally, it includes instances representing network state and information about an attacker. The main disadvantage of UCO is the inability to integrate information from different sources of the same type. On the contrary, it requires manual implementation for a specific networking system, which emerges as an obstacle to real-time security.

Motivated by the fundamental requirement of security when developing a dynamic system and the cons of existing cybersecurity ontologies, the Institute of Computer Science in Poland proposed a semantic approach for observing system components, retrieving up-to-date data about those systems and potential risks; in fact, due to the increasing number of sub-systems, as well as the physical equipment needed, the complexity of system architecture was greatly enhanced. Some of these cons include: the attempt to integrate the widest range of domains possible or a very specialized domain affecting scalability, the inability of external knowledge integration, which demands the manual effort of user and the difficulties in integrating dynamic data from real-time auditing. Thus, they propose a cybersecurity framework based on the existing dynamic cybersecurity ontology (DCO), which fills the gaps in current solutions (UCO, CVO, etc.) by implementing automatic data mining mechanisms and aggregation of results from dynamic knowledge sources (Shodan, https://www.shodan.io/ 20 November 2022, or Cencys, https://censys.io/, accessed on 20 November 2022) in a monitoring system [78]. Focusing on correlation with common vulnerabilities exposure (CVEs) and further integration with the existing ontologies, they achieve real-time data analysis, according to the needs and vulnerabilities of each networking environment.

Another cybersecurity challenge involved in IoT, is the distinct security mechanisms of each interconnected domain, which leads to lack of knowledge of basic elements of their components (assets, vulnerabilities, threats, etc.). This issue is tackled in the work of Bruno Augusti Mozzaquatro et al. [50]. The existence of numerous and heterogeneous devices in IoT allows adversaries to exploit, very often, common and known vulnerabilities. The basic idea of the authors is the integration of these well-known vulnerabilities in a cybersecurity framework for an existing ontology (IoTsec, https://github.com/brunomozza/IoTSecurityOntology/blob/master/iotsec.owl, accessed on 20 November 2022), utilizing knowledge reasoning. This ontology-based cybersecurity framework is separated in three layers, i.e., the design time, the run time, and the integration layer used by the two others. In the first layer, existing security services are reused, in order for the user to implement security mechanisms according to the needs of the network environment. In the second layer, monitoring mechanisms gather security alerts from other security tools (firewalls, vulnerability scanners, etc.) and each security alert/incident is evaluated to discover effective solutions to improve or recover, this specific time, the network system.

The third layer provides cybersecurity information by deriving information from pre-build cybersecurity services from IoTsec ontology. By implementing the proposed method in a realistic scenario (Wi-Fi vulnerabilities), the ontology identified a service (WPA2—Wi-Fi Protected Access protocol) and proposed specific solutions, based on the SPARQL query. The main issue remained the uncertainty of cybersecurity attacks ("zero-day" attacks), which allow adversaries to stay undetected.

Real-time security should be preceded by interoperability, especially security updates, because even "zero-day" attacks become useless when an operating system is patched (updated to a more secure version); in fact, according to the Ponemon Institute, 80% of successful breaches are due to zero-day vulnerabilities [66]. Implementing semantics related to security patterns [79], and automating the classification of threats and vulnerabilities, as well as countering these attacks via semantic modeling, support the foundation of a robust cybersecurity system.

4.1.3. Data and Information Modeling for UUVs

As already mentioned, the volume and variety of data generated from numerous and heterogeneous sensors are key challenges, in addition to the issues related to the water as a medium of transmission, and to many other cybersecurity issues that are emerging. To overcome such issues in an efficient and effective way, the key is the design of approaches followed by engineers for the data and information modeling. Information modeling mainly concerns the "representation of concepts and the relationships, constraints, rules and operations to specify data semantics for a chosen domain of discourse" [80]. Specifically, information modeling supports the organization by facilitating accessibility and reuse of content with various and innovative ways. The result of efficient and effective information modeling approaches is the delivery of an open, reusable, validated and evaluated information model, which is a formal description of the information needs of a group of users [81]. Thus, the modeling of information needed by users/actors/agents to interoperate in IoUT environments, in which the information generated by underwater assets is vast and heterogeneous, must be taken into serious consideration. Several challenges are encountered during data modeling, and mainly concern big data (the four Vs) and its characteristics. Furthermore, data quality, information quality, and the computation complexity of vast numbers of heterogeneous data, affect enormously the results [82].

IoUT must support the sharing of information between assets in a time- and energy-efficient manner. The design of a hierarchical information system is undoubtedly essential in order to keep a smooth flow of data/information in the UWSN. Members of the Department of Electronic Engineering of Tsinghua University, Beijing, China, proposed a system for hierarchical information acquisition as well as a flowchart for the collection scheme of UUV/AUVs or other interoperating assets [83]. Thus, depending on which state of the chart the asset is at, it makes decisions for the number of channels that will be used, or decisions for the time the gathering of information should be established; this process is considering energy-efficiency as the principal factor. Simulation experiments confirmed the efficiency of the proposed algorithm.

In addition, information exchange in the IoUT setting, especially in SARs and military operations, should be extremely precise and succinct, containing only the necessary information for the leader of UUV/AUV or shore platform to act promptly and coordinate the swarm efficiently. Localization is the initial task in order to further extend the capabilities of an unmanned vehicle. In related work [84], a method for localization is proposed based on error ellipse for UUVs/AUVS geometric interpretation and intuitiveness. The idea is that the leader (master UUV/AUV) carries high-precision sensors, sending highly accurate data to the rest of vehicles (slaves) in order to be able to correct their position accordingly, due to their low-precision sensors.

Visually represented information is also necessary for commanders to have a picture/view of the environment where the vehicles move, but also to support the adaptive decision process of the vehicle itself. Related work presents an adaptive visual information gathering (AVIG) framework for underwater autonomous vehicles, in order to enhance their various capabilities such as positioning, navigation and object recognition [65]. The work has been motivated by the difficulties emerging in deep waters, making direct communication between an operator and an underwater robot impossible. Utilizing semantics, a convolutional neural network (CNN) for semantic image segmentation and algorithms for environmental modeling, the proposed work has been integrated in a ROS (robotic operating system) environment.

Collecting and analyzing environmental data and information is also a key factor in IoUT, to have an operational advantage (over the enemy, i.e., human or physical phenomena). More specifically, NATO CMRE's EKOE reports that this is critical especially in underwater environments, where this knowledge offers an advantage in undetected vehicles, as well as for the early detection of the enemy [85]. Reaching environmental awareness at high levels supports more efficient prediction and decision-making tasks executed by commanders, but also by a UUV/AUV itself.

4.2. Cybersecurity in IoUT

From health to military industries, the race of achieving the most and most valuable information is challenging. Especially in military operations, information is the key factor which will determine the successful outcome. However, special components of information should be considered, namely the CIA triad as mentioned above. Underwater assets rely strongly on ICTs, and this leads to numerous technical vulnerabilities, which bring privacy concerns and security to the forefront [44]. Implementing an information security system or an intrusion detection system is not auxiliary, it is mandatory.

Establishment of a robust security underwater network architecture demands two prerequisites, i.e., determination of security requirements and comprehension of adversaries' strategy to exploit a vulnerability. Accordingly, the adoption of a real-time monitoring concept extends the effectiveness of cyber-defenses and supports early alerts. Threat modeling and risk assessment are key solutions to counter these challenges. They can offer both prediction and rapid evaluation of system vulnerabilities. Andrei Brazhuk et al. [86], with the aim to provide solutions to above issues, built an ontology-based model, which integrates well-known datasets (CVE, ATT&CK, etc.) in OWL and RDF formats. In consequence, relations between attack techniques, attack patterns, weaknesses and vulnerabilities are described, to decrease security vulnerabilities.

An interesting work about a dynamic risk assessment in autonomous ships is presented in [87]. Interconnection of vast number of sensors, as well as overwhelming computations, increase complexity, which have consequently expanded the attack surface. With the aim to provide cyberattack scenarios, related to the navigation and propulsion systems, based on identified vulnerabilities, two methods are incorporated, i.e., Formal Safety Assessment (FSA), for ranking hazardous scenarios and Cyber Preliminary Hazard Analysis (CPHA), to conduct threat assessment for autonomous vessels.

Wormhole [18,55], a routing attack, in which malicious or compromised node eavesdrops data packets from nearby friendly assets and redistributes them to the attacker's host, can be devastating. Dargah et al. [88], present an approach to detect and mitigate wormhole attacks in a UWSN. More specifically, they propose a cooperative detection strategy, in which each node discovers its neighbors through a secure discovery protocol. Their approach is divided into three distinct phases i.e., discovery, silent monitoring, and detection. During the second phase, receiver nodes extract a hash-based signature and reply with report packets containing its ID and the time stamp of the signature, confirming their identity. After executing simulation experiments in OMNET++ (https://omnetpp.org/, accessed on 20 November 2022), they validated their model.

Traditional routing schemes differ from these in IoUT. Propagation of acoustic signals in water does not allow the integration of terrestrial routing protocols. However, depth can facilitate this challenge. More specifically, in [89], a depth-based secure routing (DBSR) protocol is proposed, based on the most widely used routing protocol in underwater sensor networks, i.e., depth-base routing protocol (DBR), which requires solely the depth information of assets to operate [90]. DBSR broadens its capabilities by implementing distinct steps to enhance security. In particular, before initial communication, each node possesses its own key along with a public key, to use them for verification. Although the general concept of a pair of keys is widely incorporated by IT systems, energy limitations in underwater world can be crucial. Therefore, elliptic-curve cryptography (ECC)-based algorithms were utilized, to decrease the overall overhead of nodes.

Finally, a very common method for attack mitigation, is the deployment of honeypots Thus, organizations protect their real systems from external threats, by attracting adversaries and determining their strategy [91]. Honeypots are usually placed near the assets they are attempting to mimic. An interesting survey for honeypots in IoT is presented in [92], presenting a basic honeypot architecture, known as honeynet. Honeypots and honeynets can be classified in various categories based on their purpose, role, level of interaction, scalability, etc. This method is applicable in IoT and can be integrated by IoUT in several ways. Suratkar et al. [91] present an interesting approach of an adaptive honeypot concept which, through a Q-learning method, supports the functionality of firewalls, and other security mechanisms for severity analysis. Furthermore, in [93], dynamic interaction of a honeynet through reinforcement learning is proposed, resulting in risk analysis and adaptive security policies for effective automated decisions related to risk, cost, and time factors.

Even though security mechanisms become constantly more sophisticated, the main challenge of cyber warfare remains, i.e., the precedence of cyber adversaries. Every protective asset is vulnerable to be compromised or avoided. Therefore, the probability factor should be a principal component in defending strategies. Issue of uncertainty in both domains, cybersecurity and IoUT, can be taken as an advantage, by incorporating semantic knowledge and reasoners. Strong interoperability between underwater assets, such as UUVs and nodes, in combination with a robust security system can give early alerts about potential exploitation.

4.3. Simulation of Cybersecurity and Interoperability in IoUT

Assuming that an underwater network has been established taking into consideration the cybersecurity and interoperability aspects, we should be able to ensure its robustness, effectiveness, and operability. Simulation software allows engineers and scientists to predict the outcome of operational scenarios using data from the real-world. For example, companies take advantage of simulation software to design their products in the digital world, without the need for repetition of expensive and time-consuming physical representations. To realize the benefits of simulation, we can think of the designing of a UUV/AUV with specific requirements and characteristics, based on the hazardous environment it operates in. Simulation engineers can change environmental conditions unlimited times in a protected and monitored area, in order to measure its durability in various situations or to reach the limits of the system's endurance and extract quickly, accurately and cost-efficiently, its failure points. Especially in the IoUT domain, where danger is a major factor, and heterogeneity exists in plethora, simulation facilitates procedures tremendously, without affecting the accuracy of results. In this review, we mainly focus on the simulation of trajectories of UUVs/AUVs and their cooperation, as well as on the cybersecurity issues that appear. To achieve efficient simulation in different domains, several tools need to be available. Co-simulation of these tools is a very challenging research topic, due to their heterogeneity. Co-simulation is the joint simulation of loosely coupled stand-alone sub-simulators, taking into consideration their heterogeneity [94].

One of the goals of our research is to simulate the underwater environment in which underwater assets will interoperate, as well as assets' communication. Qualnet Network Simulation Software (https://www.scalable-networks.com/products/qualnet-network-simulation-software, accessed on 20 November 2022) is a scalable simulation tool for replicating live networks; it is used for commercial and military purposes, as well as by governments and educational organizations around the world. In addition, Qualnet provides a wide range of libraries and popular protocols, such as the Military and Radios library and Network (ARP, IPv4) and internet protocols (FTP, HTTP). It can run accurate simulations and analyze networks efficiently. This tool is utilized in related work [95], in which the simulation of an SDN (https://sdn.ieee.org/outreach/resources, accessed on 20 November 2022) IoUT was successfully established. Furthermore, it can model numerous nodes and supports the designing of new protocol models and the optimization of existing models. WOSS (World Ocean Simulation System, http://telecom.dei.unipd.it/ns/woss/, accessed on 20 November 2022) is another open-source simulation tool, developed in C++, which enables the integration of existing underwater channel simulator (NS-2, https://ns2simulator.com/ns2-download/ 20 November 2022, NS-3, https://ns3simulation.com/network-simulator-software/, accessed on 20 November 2022, etc.); the user can input environmental data and as an output can have a channel realization. Aqua-Sim (https://github.com/rmartin5/aqua-sim-ng, accessed on 20 November 2022), an open-source underwater simulator which supports a vast number of protocols and features, provides simulation of acoustic signals and packet collisions in UWSNs, as well as a three-dimensional deployment. This simulation tool is the most widely utilized by researchers and it is based on the famous NS-2 (Network Simulator) tool, which is written also in C++ and is highly suitable for UWSNs. Its association with a visual tool, and support of monitoring node placement, movement, and packet flow, allow users even more complex experimentation [96]. Another well-known simulation tool is SUNRISE (Sensing, Monitoring and Actuating) [97]; it is an environment-based testbed for UWSN, designed by La Sapienza University. It supports scalability and heterogeneity across various domains and real-time environments. Its main advantage over the rest of the tools is its ability to span different types of underwater environments in various locations. In addition, the SUNRISE2SUNSET plug-in [97] allows users to simulate, emulate and test novel underwater systems (at-sea). Additionally, OMNeT++ is a very simple but effective, extensive, modular simulation library and framework for building network simulators. It provides an excellent programming guide and has a library of simulation classes [98]. Numerous and various protocols are supported and provide a GUI (graphical user interface) for execution. The UDMSim simulation platform was developed to support a data mulling-oriented solution. This tool merges the AUV Motion and Localization (AML) simulator and NS-3 [99] and is capable of reproducing realistic scenarios with localization errors and providing evaluation of underwater communications, by simulating the signal and connection losses during an operation. GloMoSim (global mobile information system simulator) is another simulation tool which provides scalability to networks with a vast number of heterogeneous devices. It supports a vast number of networking protocols, both for wired and wireless networks. The main disadvantages of this tool are the poor documentation, and its rare updates. Lightweight simulation and detailed visualization are two main advantages of TOSSIM (https://networksimulationtools.com/tossim-in-wsn/, accessed on 20 November 2022), a discrete event simulator. It provides a powerful GUI and supports a wide range of network interactions. Furthermore, it provides a simple yet mighty emulator for WSNs (wireless sensor networks). While TOSSIM can be utilized for fast and representative results, its lack of accuracy in real-world results and several self-made assumptions of this tool, can be important deterrents for its selection. Routing schemes in communication can be very complex. Finally, a network emulation software which provides huge capabilities and realistic environment to network and security professionals is EVE-NG (emulated virtual environment next generation, https://www.eve-ng.net/, accessed on 20 November 2022). It supports cloud networking and over 1000 nodes per simulation. In addition, it allows users to extract information about the quality bandwidth, delay, jitter, and loss characteristics of communications. Table 3 presents general information of the experimented simulation tools and Table 4 provides their comparison based on specific features.

Table 3. Comparison of network simulation tools based on general information.

Name of Tool	Programming Language	Easy to Use	Heterogeneity Support	GUI Support	Documentation Availability
WOSS [100]	NS-3-based, C++	Medium	High	No	Yes
AQUA-Sim [96]	NS-2-based	High	Medium	Yes	Yes
NS-2 [101]	C, C++, OTcl	High	High	Limited	Yes
NS-3 [101]	C++ (optional Python bindings)	Medium	High	Yes	Yes
SUNRISE [97]	NS-2-based	Medium	High	No	Yes
OMNeT++ [98]	C++	High	Medium	Yes	Limited
UDMSim [99]	NS-3-based, AML	Medium	High	No	Limited
Gazebo [102,103]	C++	Medium	High	Yes	Excellent
QualNet [95]	C++	Medium	Medium	Yes	Excellent
GloMoSim [104]	C	Low	Medium	Limited	Limited
TOSSIM [105]	Python, C++	High	Medium	Yes	Yes
EVE-NG [106]	Python, Java and Ansible libraries	High	High	Yes	Yes

Table 4. Comparison of network simulation tools based on properties of simulation.

Name of Tool	Network Support Type	Protocol Injection	Number of Nodes	Additional Functionalities
WOSS	Wireless Sensor, Underwater	Yes	-	Integration of any existing underwater channel simulator with environmental data as input
AQUA-Sim	Wireless Sensor, Underwater	Yes	-	Accuracy in environmental conditions (wind, current, waves, etc.)
NS-2	Wired/Wireless Sensor, Underwater	Yes	<3000	Protocol simulation, configuration of network entities, event logging
NS-3	Wired/Wireless Sensor, Underwater	Yes	Unlimited	Multi-tier heterogeneous network, PCAP format, variety of modules
OMNeT++	Wireless, Underwater	Yes	-	Real-time simulation, database integration
UDMSim	Wired/Wireless Sensor, Underwater	Yes	-	Trace-based network simulation with NS-3
Gazebo	Wired/Wireless Sensor, Underwater	Yes	Unlimited	Extensive set of sensors, models and plug-ins, and ROS integration
QualNet	Wireless Sensor, Underwater	Yes	<20,000	Illustration of security models (eavesdropping, DoS attack, etc.)
GloMoSim	Wired/Limited Wireless, Underwater	Yes	<10,000	Offers standard APIs
TOSSIM	Wireless sensor network emulation	Yes	<1000	Powerful and lightweight simulation
EVE-NG	Wired/Wireless sensor networks, Software Defined Network, Cloud	Yes	>1000	Huge capabilities even in the commercial version, but even more in paid version

As presented in this review, security is linked to interoperability, and therefore we should be able to simulate both types of issues in an underwater network. With the aim to propose a simulation environment for interoperability issues and cyberattacks that compromise communication by gaining control of data flow (packet sniffing), a related work presents the open-source PyPower tool (https://github.com/rwl/PYPOWER/, accessed on 20 November 2022) [107]. PyPower is a project developed in Python, providing a Power-Attack simulation engine which captures the behavior of components in the protection layer. As mentioned in previous sections, another dangerous cyberattack that can demolish a communication network is a DoS or DDoS attack. In related work [108], a powerful networking tool is represented under the name Graphic Network Simulator 3 (GNS3), for modeling DDoS attacks; GNS3 is a well-known tool for the network engineering domain. It comes with a free and commercial license. The advantage of GNS3 is that virtual and real devices are combined easily in order to simulate attacks, such as packet traffic in NS-2 simulator. Another effective framework for cyber-security tasks and dynamic scenario design is HackIt (https://github.com/marcan/hackit, accessed on 20 November 2022) This is an open-source tool developed mainly in Python2 (https://www.python.org/download/releases/2.0/, accessed on 20 November 2022) and Flask (https://flask.palletsprojects.com/en/2.2.x/, accessed on 20 November 2022), with many essential features such as network nodes, strategies, and commands [109]. The interesting part is that it is suitable to simulate deception scenarios such as honeypots, to lure cyber-adversaries and investigate hackers' decisions. More specifically, in related work [110], a real-world scenario was simulated; the objective was to steal credit card information from a web server by sniffing network's traffic. To counter these assaults, they have inserted deceptive servers in the architecture, acting as honeypots and involved human participants to exploit the network. HackIt facilitates the extraction of very useful information about this method of deception, supporting the cybersecurity domain in a network environment with real human attackers. Another powerful simulation tool is Foreseeti (https://foreseeti.com/, accessed on 20 November 2022). Its AI-based predictive cyberattack simulation functionality supports users to automate threat mitigation and risk assessment and identify fast and accurately incoming cyber threats. It provides cloud simulation capability as well as custom scenario-based attack simulations. Moreover, its ability to recommend the implementation of new security mechanisms to existing vulnerabilities, allows users to reduce the attack surface. Infection Monkey (https://github.com/guardicore/monkey, accessed on 20 November 2022) is an agent-based attack simulation tool designed to test networks. The ease of configuration and the broad pool of libraries for manual configuration allow analysts to decide on new security implementations accurately and efficiently. Its main disadvantage is that the extracted information is presented after the completion of the attack. A powerful simulation tool, developed mainly for Active Directory (AD, https://en.wikipedia.org/wiki/Active_Directory, accessed on 20 November 2022) reconnaissance, is BloodHound (https://github.com/BloodHoundAD/BloodHound, accessed on 20 November 2022). It is a JavaScript web application providing a built-in database, and users can utilize it to identify and unveil attack paths in order to counter vulnerabilities. Moreover, the MITRE Attack Framework is a globally accessible knowledge base for adversary strategies, used for the development of threat models in numerous organizations and security community [111]. Several cyber security frameworks are built on this, such as the CALDERA (https://github.com/mitre/caldera/, accessed on 20 November 2022); an open-source active research project by MITRE. It provides a plethora of separate repositories in order to extend its capabilities and utilize it in specific cases involving both offensive (red) and defensive (blue) operations [112]. Finally, NeSSi2 (Network Security Simulator, http://www.nessi2.de/index.html, accessed on 20 November 2022) is a network simulation tool which was developed exclusively for security purposes. With a variety of features, as well as detection algorithm plug-ins, it is used for security search and evaluation purposes [113], offering distributed simulation to reduce time of process. Scalability, fidelity, and extensibility are the main benefits of this framework, facilitating integration of applications, importation of a network topology or its automatic creation and cooperation with third-party software such as the well-known Wireshark (https://www.wireshark.org/docs/, accessed on 20 November 2022) [114]. Table 5 provides a brief comparison of experimented cybersecurity simulation tools.

Table 5. Comparison of security simulation tools.

Tool	Attack Variety	Realism	Advantages	Disadvantages
GridAttack Sim [115]	Medium	Medium	Co-simulation with NS-3, detailed report analysis, simple GUI	Designed mainly for surface smart grid topologies
Foreseeti [116]	High	High	Powerful visualization, detailed analysis report and probabilistic feature which recommends implementation of security mechanisms	Two licenses, commercial one has limited features
GNS-3 [106]	High	High	Design of complex network topologies, real-time packet capture, connection of the simulated world to the real world	Two licenses, commercial one has limited features
HackIt [109,110]	High	High	Variety of protocols integration	Only command-line feature (No GUI)
Caldera [117]	High	High	Autonomous adversary emulation and incident response, choice of defender or attacker	Difficult configuration
NeSSi2 [113,114]	Medium	Medium	Manual creation of network with variety of devices	Antiquated
Infection Monkey [118]	Medium	High	Visualization of adversary moves, analysis from well-known databases (MITRE ATT&CK, Zero Trust, etc.)	Limited variety of attacks
BloodHound [119]	High	Medium	Integrated function for queries	Developed mainly for Active Directory (AD) and Azure environment

During numerous trials with underwater environment simulation tools, we have discovered another active stand-alone open-source tool, namely Gazebo (https://github.com/osrf/gazebo, accessed on 20 November 2022) [102,103]. In addition to its scalability, ease of installation and handling, it is suitable for integration with ROS. This feature allows us to represent a swarm of UUVs in a UWSN. Our plans include this extension, in order to be able to represent packet flows during communications, as well as their protocols and the integration of the SLAM (simultaneous localization and mapping) ontology [120].

In addition, a plethora of co-simulation tools exist across various domains. Open Simulation Platform (OSP, https://opensimulationplatform.com/, accessed on 20 November 2022) is an open-source initiative for co-simulation of the maritime industry. The motivation of this project is the constant growth of complexity of systems and software of ships, and other maritime/offshore assets, resulting in several difficulties in their designing. Another co-simulation method, which utilizes a bunch of tools, is presented in related work of Le et al. [121]. By combining cyber-physical components, as well as cybersecurity scenarios, it evaluates the impact of security threats of a communication network. In this procedure, a combination of network and power system simulation tools is established. In another related work [115], a co-simulation framework, called GridAttackSim is proposed, to simulate various cyber threats and their consequences in a smart grid infrastructure. The simulation output can be visualized and compared to recognize malicious behaviors and strategies of adversaries. The framework uses three different simulation tools.

Finally, the upcoming trend of our era cannot be omitted. Above IoT lies a new technology, the digital twin [122], which emerged to replace most of the simulation tools that delimited solely in the prediction functionality. New generation platforms can manage any type of virtual and physical entities interoperating in the Internet of Everything (IoE), replicate any kind of processes, predict how they will perform, and act based on these predictions towards optimizing performance and available resources. This new kind of simulation platform (sense, analyze, act) is introduced in the era of the digital twin.

5. Discussing Open Issues and Challenges

Autonomous underwater vehicles have already attracted a lot of attention, especially due to their capabilities to operate in a swarm, significantly minimizing the human factor; UUVs are making civilian and military operations tremendously easier, mitigating any ethical doubts with cost-effective vehicles. Nevertheless, the establishment of a robust and secure underwater network raises several issues. Interoperability between underwater assets is a challenging goal, due to the variety and veracity (quality of data) of data transmitted in the water. Lack of communication protocols' standardization among research institutes and organizations generates even more obstacles, by making difficult the cooperation between them and the establishment of common research foundations. Moreover, a variety of security vulnerabilities arises especially due to the complexity and uncertainty of the IoUT architecture, its vast number of assets and their heterogeneity, as well as the non-formalized domains of IoUT and cybersecurity.

Based on an extensive and systematic research of the IoUT and cybersecurity domains, we have identified and presented in this paper the need to further investigate the key issue of interoperability and standardization of communication protocols. Due to the absence of a typical communication channel and the existence of a common IoUT "language", the challenges that are emerging are numerous [85]. Critical capabilities of UUVs such as autonomous decision-making, adaptive path-planning, self-management and self-diagnosis, cannot be easily achieved, mainly due to the difficulty in information/data exchange. Furthermore, data related to a key factor of underwater missions, i.e., weather conditions, are unable to be utilized and distributed, which consequently causes the failure of an operation. A commonly agreed formal message encoding and decoding schema can be a solution towards IoUT interoperability. Alternatively, or complementarily, a tool-supported methodology for the automated alignment and translation of exchanged data and messages encoded in different syntax and semantics [123] could be a more realistic and efficient solution in the IoUT domain, allowing different stakeholders (vendors, organizations, research institutes) to keep their own data and semantic models local to their solutions.

Furthermore, a consequence which is derived from big data is recurring data, especially in dangerous military and SAR operations. During our research we distinguished the lack of a data "sieving" process. During a large-scale operation, two or more UUVs may exchange the same information with the leader, affecting the feedback to the commander and causing networking chaos. Validity of information facilitates communication in the underwater domain, allowing the distribution of high-priority data by not utilizing extra bandwidth. A distinct sensor incorporating machine learning methods, exclusively for the process of information discrimination would be very useful in operations with swarms of UUVs.

Emerging from the above issue as a rational result, but also from the principles of military operations, UUVs must act as a role-based asset. This means that every unit should be assigned its own tasks, and its sensors are dedicated to these tasks according to their capabilities. This strategy allows for the elimination of recurring information, but mainly supports the quality of information which is transmitted by the leader of the swarm to the commander. Nevertheless, non-standardization of communication protocols remains a critical obstacle, due to the heterogeneous devices every role-based UUV would possess.

Sharing knowledge between UUVs in a common machine-understandable language can be achieved through semantic knowledge presentation. Additionally, the impact of fast and trustworthy decision-making in critical situations can be easily predicted and the exchange of important information, as well as its representation, can be efficiently achieved. Nevertheless, apart from semantic modelling and simulation of interoperability issues, trustworthiness of universal interoperability which resides in cybersecurity domain, affects every interconnected device above and below the surface.

UUVs and their applications result in many vulnerabilities. Collaborative tasks and heterogeneous devices demand real-time information exchange, adding even more obstacles in establishing a secure underwater network. Although traditional operating systems differ from those in underwater communications, threats, and risks from the cybersecurity aspect, remain almost the same, with the main challenge being the protection of the CIA triad. However, countermeasures for regular WSNs are not directly applicable to UWSNs. For example, nodes, a critical asset for a robust underwater network, are the most vulnerable to cyber threats. Acting as transponders of information, they may distribute data packets for the whole operation. The eavesdropping of such communication or a DDoS attack are challenging threats that may be encountered. Moreover, as underwater assets incorporate electro-acoustic transducers to receive and transmit sound signals [124], adversaries exploit emerged vulnerabilities from a native characteristic of water, i.e., latency, which delays the distribution of this huge volume of data (and generated alerts from cyber incidents) as well as their inspection and analysis. Hence, the classification of attacks differs also. Security measures should be implemented and must be a precondition for the start of a mission. Simulations act as catalytic agents for the implementation of these measures, supporting even further the scientific community. Simulation tools are a key factor for the successful evaluation of a task.

Based on our extensive research, the lack of specifically designed simulation tools for underwater security communications with the utilization of semantic modelling, was identified. Initially, the selection of a tool should be based on specific requirements, with the most important being (a) capability of heterogeneous data integration using ontologies/semantic knowledge, (b) support of multiple UUVs (swarms) simulation, (c) support of modeling and simulation of sensors and network interfaces, and (d) support of visualization for realistic scenario representation. Furthermore, in order to reuse an existed simulation tool or develop a new one, there is a high need for important extensions to be implemented in order to be compatible with the various emerging technologies, and thus to be more efficient. As we have already proposed in our preliminary work [125], introducing a high-level architecture model, these extensions include: (i) a compatible framework for integration of semantic data in various formats, (ii) the ability to analyze and integrate the huge amount of exchanged data to extract infer new knowledge, (iii) the enrichment of such integrated knowledge with underwater protocols and libraries of cybersecurity frameworks.

The secure interconnection and interoperability between the devices and the vehicle or the vehicle and a central platform are resolved by using a semantic approach/ontology, especially if combined with a standardized middleware architecture to establish a common "language", regardless of the arrangement of heterogeneous components of IoUT.

Concluding, what is needed today is an overall integrated approach for automated threat modeling, semantic knowledge representation, and robust simulation of the cybersecurity and interoperability challenges using an ontological model, to support the efficient prediction of the impact of rapid decision-making in critical situations such as military and SAR ones.

6. Conclusions and Future Work

Although UUVs and their applications are popular in civil and military operations, the establishment of interoperability across various platforms, and the establishment of robust underwater network architectures in IoUT from a cybersecurity perspective, are key challenges. In this paper, we have presented a systematic review of methods and tools of semantic modeling and simulation for cybersecurity and interoperability on the IoUT. A number of open issues and challenges have been identified, proposing how to overcome and meet them, respectively. In general, the domain of IoUT is open for research, especially for topics related to interoperability and security.

In this line of research, we have worked on interoperability and cybersecurity issues in swarms of trustworthy UUVs in a military/search-and-rescue (SAR) setting. We have researched semantic modeling and simulation approaches that aim to facilitate commanders of military/search-and-rescue operations to effectively support critical and life-saving decision-making, while handling interoperability and cybersecurity issues on the IoUT.

A high-level architectural design of a proposed cybersecurity simulation tool has already been presented in our preliminary related work [113].

Our future plans include the implementation of such a tool, extending already existing semantic and simulation methods and tools reused for this purpose. Finally, several related ontologies have been developed or are under development by our research lab, specifically in the domains of IoT/IoT-trust (https://github.com/KotisK/IoTontos, accessed on 20 November 2022), cybersecurity for communication/network assets, drones semantic trajectories (https://github.com/KotisK/onto4drone, accessed on 20 November 2022), and digital twins (https://github.com/KotisK/SEC4DigiT, accessed on 20 November 2022). Our aim is to integrate them with existing semantic approaches of cybersecurity and underwater domain ontologies (UCO, CVO and OWO) and then utilize them in selected simulation tools.

Author Contributions: Conceptualization, S.S., C.K. and K.K.; methodology, S.S. and K.K.; software, S.S.; validation, S.S., K.K. and C.K.; formal analysis, S.S. and K.K.; investigation, S.S. and K.K.; resources, S.S.; data curation, S.S.; writing—original draft preparation, S.S.; writing—review and editing, K.K. and C.K.; supervision, K.K.; project administration, K.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

Abbreviation	Definition	Abbreviation	Definition
ACO	Ant Colony Optimizaiton	IoUT	Internet of Underwater Things
AD	Active Directory	ISO	International Organization for Standardization
AML	AUV Motion and Localization	LSS	Large Scale Service
AoA	Angle of Arrival	MARL	Multi-Agent Reinforcement Learning
ARP	Address Resolution Protocol	MEBN	Multi-Entity Bayesian Network
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge	NATO	North Atlantic Treaty Organization
AUV	Autonomous Underwater Vehicle	NeOn	Networked Ontologies
AVIG	Adaprive Visual Information	NeSSi	Network Security Simulator
C2	Command and Control	NIST	National Institute of Standards and Technology
CA	Climate Analysis	NOAA	National Oceanic and Atmospheric Administration’s National Weather Service
CCE	Common Configuration Enumeration	NS	Network Simulator
CDO	Climate Data Online	NUWCDIVNPT	Naval Undersea Warfare Center Division Newport
CIA	Confidentiality, Integrity, Availability	OSI	Open Systems Interconnection
CMRE	Center for Maritime Research and Experimentation	OSP	Open Simulation Platform
CNN	Convolutional Neural Network	OWASP	Open Web Application Security Project
CPHA	Cyber Preliminary Hazard Analysis	OWC	optical wireless communication
CVE	Common Vulnerabilities and Exposure	OWL	Web Ontology Language
CVO	Cybersecurity Vulnerability Ontology	OWO	Open World Ontology
DBR	Depth-Based Routing protocol	PSO	Particle Swarm Optimization
DBSR	Depth-Based Secure Routing protocol	RDF	Resource Description Framework
DCO	Dynamic Cybersecurity Ontology	RDFS	Resource Description Framework Schema
DDoS	Distributed Denial of Service	ROS	Robot Operating System
DKOE	Data Knowledge and Operational Effectiveness	ROV	Remotely Operated Vehicle
DoS	Denial of Service	SAR	Search-and-Rescue

DUNE	Distributed Unified Navigation Environment	SDN	Software Defined Network
ECC	Elliptic-Curve Cryptography	SLAM	Simultaneous Localization And Mapping
ENISA	European Network and Information Security Agency	SOA	Service Oriented Architecture
EVA	Efficient Void Aware	SPARQL	SPARQL Protocol and RDF Query Language
EVE-NG	Emulated Virtual Environment Next Generation	SSC	Software to Software
FSA	Formal Safety Assessment	SSN	Semantic Sensor Network
FTP	File Transfer Protocol	STANAG	Standardization Agreement
GEBCO	General Bathymetric Chart of the Oceans	STIX	Structured Threat Information eXpression
GloMoSim	Global Mobile Information System Simulator	STO	Science and Technology Organization
GNS	Graphic Network Simulator	SWRL	Semantic Web Rule Language
GUI	Graphical User Interface	ToA	Time of Arrival
HTTP	Hypertext Transfer Protocol	UCO	Unified Cybersecurity Ontology
HTTPS	Hypertext Transfer Protocol Secure	USV	Unmanned Surface Vehicle
ICT	Information and Communication Technologies	UUV	Unmanned Underwater Vehicle
IDA	intelligent data analytics	UWAN	Underwater Wireless Acoustic Network
IDS	Intrusion Detection System	UWCN	Underwater Wireless Communication Network
IoC	Indicator of Compromise	UWSN	Underwater Wireless Sensor Network
IoE	Internet of Everything	W3C	World Wide Web Consortium
IoTSEC	Internet of Things Security	WASC	Web Application Security Consortium

References

1. Eca Group. News & Stories. Available online: https://www.ecagroup.com/en/news-stories (accessed on 3 October 2022).
2. France, B. *Interim Report n°3 on the Accident on 1st June 2009 to the Airbus A330-203 Registered F-GZCP Operated by Air France Flight AF 447 Rio de Janeiro—Paris*; BEA Bureau of Enquiry and Analysis for Civil Aviation Safety: Le Bourget, France, 2011.
3. Armed and Intelligent—Global Defence Technology. Issue 91. 2018. Available online: https://defence.nridigital.com/global_defence_technology_sep18/issue_91 (accessed on 4 October 2022).
4. The Four V's of Big Data—Enterprise Big Data Framework©. Available online: https://www.bigdataframework.org/the-four-vs-of-big-data/ (accessed on 4 October 2022).
5. Liu, F.; Tang, H.; Qin, Y.; Duan, C.; Luo, J.; Pu, H. Review on Fault Diagnosis of Unmanned Underwater Vehicles. *Ocean. Eng.* **2022**, *243*, 110290. [CrossRef]
6. Hernandez Corbato, C.; Milosevic, Z.; Olivares, C.; Rodriguez, G.; Rossi, C. Meta-control and self-awareness for the UX-1 autonomous underwater robot. In *Advances in Intelligent Systems and Computing*; Springer: Berlin/Heidelberg, Germany, 2020; Volume 1092, pp. 404–415.
7. The UX-1 Robot. Available online: https://www.unexmin.eu/the-project/the-ux-1-robot (accessed on 4 October 2022).
8. Chandrasekhar, V.; Seah, W.K.; Choo, Y.S.; Ee, V. Localization in underwater sensor networks-survey and challenges. In Proceedings of the 1st Workshop on Underwater Networks, WUWNET 2006, Los Angeles, CA, USA, 25 September 2007.
9. Costanzi, R.; Fenucci, D.; Manzari, V.; Micheli, M.; Morlando, L.; Natale, D.; Stifani, M.; Tesei, A.; Caiti, A. *At-Sea NATO Operational Experimentation with Interoperable Underwater Assets Using Different Robotic Middlewares*; IOS Press: Amsterdam, The Netherlands, 2018.
10. CMRE_AR_2021M. Available online: https://www.cmre.nato.int/research/publications/other-publications/1653-cmre-ar-2021m (accessed on 20 November 2022).
11. Yan, Z.; Wu, Y.; Du, X.; Li, J. Limited Communication Consensus Control of Leader-Following Multi-UUVs in a Swarm System under Multi-Independent Switching Topologies and Time Delay. *IEEE Access* **2018**, *6*, 33183–33200. [CrossRef]
12. Petritoli, E.; Cagnetti, M.; Leccese, F. Simulation of Autonomous Underwater Vehicles (AUVs) Swarm Diffusion. *Sensors* **2020**, *20*, 4950. [CrossRef] [PubMed]
13. Hu, Z.; Wang, Z.; Yin, Y. Research on 3D global path planning technology for UUV based on fusion algorithm. *J. Phys. Conf. Ser.* **2021**, *1871*, 012128. [CrossRef]
14. Gazis, A. What Is IoT? The Internet of Things Explained. *Acad. Lett.* **2021**, *1003*, 1–8. [CrossRef]
15. Menaka, D.; Gauni, S.; Manimegalai, C.T.; Kalimuthu, K. Vision of IoUT: Advances and Future Trends in Optical Wireless Communication. *J. Opt.* **2020**, *49*, 494–509. [CrossRef]
16. Fattah, S.; Gani, A.; Ahmedy, I.; Idris, M.Y.I.; Hashem, I.A.T. A Survey on Underwater Wireless Sensor Networks: Requirements, Taxonomy, Recent Advances, and Open Research Challenges. *Sensors* **2020**, *20*, 5393. [CrossRef]
17. Domingo, M.C. An Overview of the Internet of Underwater Things. *J. Netw. Comput. Appl.* **2012**, *35*, 1879–1890. [CrossRef]
18. Yisa, A.G.; Dargahi, T.; Belguith, S.; Hammoudeh, M. Security Challenges of Internet of Underwater Things: A Systematic Literature Review. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4203. [CrossRef]
19. Mary, D.R.K.; Ko, E.; Kim, S.G.; Yum, S.H.; Shin, S.Y.; Park, S.H. A Systematic Review on Recent Trends, Challenges, Privacy and Security Issues of Underwater Internet of Things. *Sensors* **2021**, *21*, 8262. [CrossRef]

20. Arul, R.; Alroobaea, R.; Mechti, S.; Rubaiee, S.; Andejany, M.; Tariq, U.; Iftikhar, S. Intelligent Data Analytics in Energy Optimization for the Internet of Underwater Things. *Soft Comput.* **2021**, *25*, 12507–12519. [CrossRef]
21. Li, J.; Wu, J.; Li, C.; Yang, W.; Bashir, A.K.; Li, J.; Al-Otaibi, Y.D. Information-Centric Wireless Sensor Networking Scheme with Water-Depth-Awareness Content Caching for Underwater IoT. *IEEE Internet Things J.* **2022**, *9*, 858–867. [CrossRef]
22. Allen, R.B. Definitions and Semantic Simulations Based on Object-Oriented Analysis and Modeling. *arXiv* **2019**, arXiv:1912.13186.
23. (PDF) NeOn Methodology for Building Ontology Networks: A Scenario-Based Methodology. Available online: https://www.researchgate.net/publication/49911337_NeOn_Methodology_for_Building_Ontology_Networks_a_Scenario-based_Methodology (accessed on 4 October 2022).
24. Wikipedia Semantic Reasoner. 2015. Available online: https://en.wikipedia.org/wiki/Semantic_reasoner (accessed on 20 November 2022).
25. Li, X.; Martínez, J.F.; Rubio, G. Towards a Hybrid Approach to Context Reasoning for Underwater Robots. *Appl. Sci.* **2017**, *7*, 183. [CrossRef]
26. European Commission. Smart and Networking UnderWAter Robots in Cooperation Meshes. *SWARMs Project. Fact Sheet. H2020. CORDIS*. Available online: https://cordis.europa.eu/project/id/662107 (accessed on 4 October 2022).
27. Liu, X.; Wang, J.; Li, W. A Formal Definition on Ontology Integration. *IET Conf. Publ.* **2012**, *2012*, 66–68. [CrossRef]
28. Lane, D.; Brown, K.; Petillot, Y.; Miguelanez, E.; Patron, P. An Ontology-Based Approach to Fault Tolerant Mission Execution for Autonomous Platforms. *Mar. Robot. Auton.* **2013**, *9781461456599*, 225–255. [CrossRef]
29. *Std 610.12-1990(R2002)*; IEEE Standard Glossary of Software Engineering Terminology. The Institute of Electrical and Electronics Engineers: New York, NY, USA, 1990; pp. 1–88.
30. Wang, W.; Tolk, A.; Wang, W. The levels of conceptual interoperability model: Applying systems engineering principles to M&S. In Proceedings of the 2009 Spring Simulation Multiconference, San Diego, CA, USA, 22 March 2009.
31. Kotis, K.I.; Pliatsios, A.; Goumopoulos, C.; Kotis, K. A Review on IoT Frameworks Supporting Multi-Level Interoperability-The Semantic Social Network of Things Framework. *Int. J. Adv. Internet Technol.* **2020**, *13*, 46–64.
32. Braga, J.; Martins, R.; Petrioli, C.; Petroccia, R.; Picari, L. Cooperation and networking in an underwater network composed by heterogeneous assets. In Proceedings of the OCEANS 2016 MTS/IEEE Monterey, OCE 2016, Monterey, CA, USA, 19–23 September 2016; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2016.
33. Gazis, V.; Goertz, M.; Huber, M.; Leonardi, A.; Mathioudakis, K.; Wiesmaier, A.; Zeiger, F. Short Paper: IoT: Challenges, projects, architectures. In Proceedings of the 2015 18th International Conference on Intelligence in Next Generation Networks, ICIN 2015; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2015; pp. 145–147.
34. Noura, M.; Atiquzzaman, M.; Gaedke, M. Interoperability in Internet of Things: Taxonomies and Open Challenges. *Mob. Netw. Appl.* **2019**, *24*, 796–809. [CrossRef]
35. Lepage, K.D.; Goldhahn, R.; Alves, J.; Strode, C.; Braca, P.; Ferri, G.; Munafo, A.; Oddone, M.; Sildam, J.; Baralli, F.; et al. Autonomous networked anti-submarine warfare research and development at CMRE. In Proceedings of the MTS/IEEE OCEANS 2015—Genova: Discovering Sustainable Ocean Energy for a New World, Genova, Italy, 18–21 May 2015. [CrossRef]
36. Alves, J.; Furfaro, T.; Lepage, K.; Munafò, A.; Pelekanakis, K.; Petroccia, R.; Zappa, G. *Moving JANUS Forward: A Look into the Future of Underwater Communications Interoperability*; The Centre for Maritime Research and Experimentation (CMRE): La Spezia, Italy, 2017.
37. Potter, J.; Alves, J.; Green, D.; Zappa, G.; Nissen, I.; McCoy, K. The JANUS underwater communications standard. In Proceedings of the 2014 Underwater Communications and Networking, UComms 2014, Sestri Levante, Italy, 3–5 September 2014; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2014.
38. NATO—News: A New Era of Digital Underwater Communications, 27 April 2017. Available online: https://www.nato.int/cps/en/natohq/news_143247.htm (accessed on 4 October 2022).
39. Baghdady, J.; Incze, M.; Dias, P.; Lima, K.; Trimble, A.Z.; Hafner, N.; Andrade, R.; Costa, M.; Ribeiro, M.; Sousa, J.; et al. Enabling interoperability among disparate unmanned vehicles via coordinated command, control, and communications strategies. In Proceedings of the 2020 Global Oceans 2020: Singapore—U.S. Gulf Coast, Biloxi, MS, USA, 5–30 October 2020; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2020.
40. Semantic Interoperability—Wikipedia. Available online: https://en.wikipedia.org/wiki/Semantic_interoperability (accessed on 4 October 2022).
41. Lakka, E.; Petroulakis, N.E.; Hatzivasilis, G.; Soultatos, O.; Michalodimitrakis, M.; Rak, U.; Waledzik, K.; Anicic, D.; Kulkarni, V. End-to-End Semantic Interoperability Mechanisms for IoT. In Proceedings of the 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Limassol, Cyprus, 11–13 September 2019; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2019.
42. Khasawneh, A.M.; Altalhi, M.; Kumar, A.; Aggarwal, G.; Kaiwartya, O.; Khalifeh, A.; Al-Khasawneh, M.A.; Alarood, A.A. An Efficient Void Aware Framework for Enabling Internet of Underwater Things. *J. Mar. Sci. Eng.* **2021**, *9*, 1219. [CrossRef]
43. LinkedIn. Top Trending Technology Domains of the Decade. Available online: https://www.linkedin.com/pulse/top-trending-technology-domains-decade-vignesh-pillai/ (accessed on 18 November 2022).
44. Kalloniatis, C.; Kavroudakis, D.; Polidoropoulou, A.; Gritzalis, S. Designing Privacy-Aware Intelligent Transport Systems: A Roadmap for Identifying the Major Privacy Concepts. *Int. J. Appl. Geospat. Res.* **2019**, *10*, 73–91. [CrossRef]
45. North Atlantic Treaty Organisation NATO. NMIOTC 3000 NSC-74/ser.: NU 120. In Proceedings of the 3rd NMIOTC Cyber Security Conference—'Food for Thought', Souda Bay, Chania, Greece, 2 August 2019. Available online: https://nmiotc.nato.in

t/wp-content/uploads/2020/01/3000-NSC-74_NU120_02-08-19_NMIOTC-2019-cyber-security-FFT-Paper.pdf (accessed on 20 November 2022).

46. The Five Biggest Cyber Security Trends in 2022. Bernard Marr. Available online: https://bernardmarr.com/the-five-biggest-cyber-security-trends-in-2022/ (accessed on 4 October 2022).
47. Cost of a Data Breach 2022. IBM. Available online: https://www.ibm.com/reports/data-breach (accessed on 4 October 2022).
48. ENISA Threat Landscape 2021—ENISA. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (accessed on 4 October 2022).
49. AIDA Project. Available online: https://www.project-aida.eu/ (accessed on 4 October 2022).
50. Mozzaquatro, B.A.; Agostinho, C.; Goncalves, D.; Martins, J.; Jardim-Goncalves, R. An Ontology-Based Cybersecurity Framework for the Internet of Things. *Sensors* **2018**, *18*, 3053. [CrossRef] [PubMed]
51. Jacq, O.; Laso, P.M.; Brosset, D.; Simonin, J.; Kermarrec, Y.; Giraud, M.-A. *Maritime Cyber Situational Awareness Elaboration for Unmanned Vehicles*; HAL: Lyon, France, 2019.
52. Pantazopoulos, P.; Haddad, S.; Lambrinoudakis, C.; Kalloniatis, C.; Maliatsos, K.; Kanatas, A.; Varadi, A.; Gay, M.; Amditis, A. Towards a security assurance framework for connected vehicles. In Proceedings of the 19th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2018, Chania, Greece, 12–15 June 2018; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2018.
53. International Maritime Organization. *Revised Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process*; International Maritime Organization: London, UK, 2018.
54. White Paper Excerpt: Leveraging ISA 62443-3-2 For IACS Risk Assessment and Risk Related Strategies. Available online: https://gca.isa.org/blog/white-paper-excerpt-leveraging-isa-62443-3-2-for-iacs-risk-assessment-and-risk-related-strategies (accessed on 7 October 2022).
55. Network Sniffing—Attackics. Available online: https://collaborate.mitre.org/attackics/index.php/Technique/T0842 (accessed on 8 October 2022).
56. Signori, A.; Chiariotti, F.; Campagnaro, F.; Zorzi, M. A Game-Theoretic and Experimental Analysis of Energy-Depleting Underwater Jamming Attacks. *IEEE Internet Things J.* **2020**, *7*, 9793–9804. [CrossRef]
57. Azadeh, A.; Shirkouhi, S.N.; Rezaie, K. A Robust Decision-Making Methodology for Evaluation and Selection of Simulation Software Package. *Int. J. Adv. Manuf. Technol.* **2010**, *47*, 381–393. [CrossRef]
58. Global Cyber Alliance. *Cybersecurity Toolkit Tool Selection Process Overview*; Global Cyber Alliance: London, UK, 2020.
59. Migueláñez, E.; Patrón, P.; Brown, K.E.; Petillot, Y.R.; Lane, D.M. Semantic Knowledge-Based Framework to Improve the Situation Awareness of Autonomous Underwater Vehicles. *IEEE Trans. Knowl. Data Eng.* **2011**, *23*, 759–773. [CrossRef]
60. Yao, H.; Han, C.; Xu, F. Reasoning Methods of Unmanned Underwater Vehicle Situation Awareness Based on Ontology and Bayesian Network. *Complexity* **2022**, *2022*, 7143974. [CrossRef]
61. Mishra, S.K.; Sarkar, A. Service-Oriented Architecture for Internet of Things: A Semantic Approach. *J. King Saud Univ. -Comput. Inf. Sci.* **2021**, *34*, 8765–8776. [CrossRef]
62. Catherine, R.; Stephan, B.; Geraldine, A.; Daniel, B. *Semantic Web 0 (0) 1 1 IOS Press Weather Data Publication on the LOD Using SOSA/SSN Ontology*; IOS Press: Amsterdam, The Netherlands, 2020.
63. Wu, J.; Orlandi, F.; O'sullivan, D.; Dev, S. An ontology model for climatic data analysis. *arXiv* **2021**, arXiv:2106.03085.
64. Rahmati, M.; Nadeem, M.; Sadhu, V.; Pompili, D. UW-MARL: Multi-agent reinforcement learning for underwater adaptive sampling using autonomous vehicles. In Proceedings of the ACM International Conference Proceeding Series, Association for Computing Machinery, Bali Island, Indonesia, 23 October 2019.
65. Guerrero, E.; Bonin-Font, F.; Oliver, G. Adaptive Visual Information Gathering for Autonomous Exploration of Underwater Environments. *IEEE Access* **2021**, *9*, 136487–136506. [CrossRef]
66. Himri, K.; Ridao, P.; Gracias, N. Underwater Object Recognition Using Point-Features, Bayesian Estimation and Semantic Information. *Sensors* **2021**, *21*, 1807. [CrossRef]
67. Sung, M.; Kim, J.; Lee, M.; Kim, B.; Kim, T.; Kim, J.; Yu, S.C. Realistic Sonar Image Simulation Using Deep Learning for Underwater Object Detection. *Int. J. Control Autom. Syst.* **2020**, *18*, 523–534. [CrossRef]
68. Yazid, M.; Tayeb, K. Ontology-based Cyber Risk Monitoring Using Cyber Threat Intelligence. In Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 21), Vienna, Austria, 17–20 August 2021; Association for Computing Machinery: New York, NY, USA, 2021. Article 88. pp. 1–8. [CrossRef]
69. Adi, A.; Węcel, K.; Abramowicz, W. The Semantic Approach to Cyber Security. Towards Ontology Based Body of Knowledge. In Proceedings of the European Conference on Information Warfare and Security, ECCWS, Hatfield, UK, 2–3 July 2015; pp. 328–336.
70. What Are Indicators of Compromise? *Digital Guardian.* Available online: https://digitalguardian.com/blog/what-are-indicators-compromise (accessed on 5 October 2022).
71. Doynikova, E.; Fedorchenko, A.; Kotenko, I. A Semantic Model for Security Evaluation of Information Systems. *J. Cyber Secur. Mobil.* **2020**, *9*, 301–330. [CrossRef]
72. Kotenko, I.; Polubelova, O.; Saenko, I.; Doynikova, E. *The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2013; pp. 638–645. [CrossRef]
73. Syed, R. Cybersecurity Vulnerability Management: A Conceptual Ontology and Cyber Intelligence Alert System. *Inf. Manag.* **2020**, *57*, 1–17. [CrossRef]

74. Syed, Z.; Padia, A.; Finin, T.; Joshi, A.; Mathews, L. UCO: A Unified Cybersecurity Ontology. In Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence Artificial Intelligence for Cyber Security, Phoenix, AZ, USA, 12–13 February 2016; Technical Report WS-16-03. Association for the Advancement of Artificial Intelligence: Washington, DC, USA, 2016.
75. CVE. Overview. Available online: https://www.cve.org/About/Overview (accessed on 5 October 2022).
76. Common Configuration Enumeration (CCE)—FAQs. Available online: https://cce.mitre.org/about/faqs.html (accessed on 5 October 2022).
77. Liu, Z.; Sun, Z.; Chen, J.; Zhou, Y.; Yang, T.; Yang, H.; Liu, J. *STIX-Based Network Security Knowledge Graph Ontology Modeling Method*; Association for Computing Machinery (ACM): New York, NY, USA, 2020; pp. 152–157.
78. Pastuszuk, J.; Burek, P.; Ksiezopolski, B. Cybersecurity ontology for dynamic analysis of IT systems. *Procedia Comput. Sci.* **2021**, *192*, 1011–1020. [CrossRef]
79. Pereira-Vale, A.; Fernández, E.B.; Pereira Vale, A.; Fernandez, E.B. *An Ontology for Security Patterns*; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2019.
80. Information Model—Wikipedia. Available online: https://en.wikipedia.org/wiki/Information_model (accessed on 5 October 2022).
81. Bray, T.; Weinberger, D.; Trippe, B.; Guenette, D.R.; Holst, S.; Altekar, G.; Laplante, M.; Maziarka, M.; Dionne, S.G. What is an information model & why do you need one? *Gilbane Rep.* **2002**, *10*, 1–32.
82. Kang, S.; Jin, R.; Deng, X.; Kenett, R.S. Challenges of Modeling and Analysis in Cybermanufacturing: A Review from a Machine Learning and Computation Perspective. *J. Intell. Manuf.* **2021**. [CrossRef]
83. Qin, C.; Du, J.; Wang, J.; Ren, Y. A Hierarchical Information Acquisition System for AUV Assisted Internet of Underwater Things. *IEEE Access* **2020**, *8*, 176089–176100. [CrossRef]
84. Du, Z.; Wang, W.; Chai, H.; Xiang, M.Z.; Zhang, F.; Huang, Z. Configuration Analysis Method and Geometric Interpretation of UUVs Cooperative Localization Based on Error Ellipse. *Ocean. Eng.* **2022**, *244*, 110299. [CrossRef]
85. Aziz El-Banna, A.A.; Wu, K. Introduction to underwater communication and IoUT networks. In *Springer Briefs in Computer Science*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 1–8.
86. Brazhuk, A. Towards Automation of Threat Modeling Based on a Semantic Model of Attack Patterns and Weaknesses. *arXiv* **2021**, arXiv:2112.04231.
87. Bolbot, V.; Theotokatos, G.; Boulougouris, E.; Vassalos, D. *Safety Related Cyber-Attacks Identification and Assessment for Autonomous Inland Ships Computational Investigation of a Large Marine Two-Stroke Dual Fuel Engine View Project FLOWMART View Project Safety Related Cyber-Attacks Identification and Assessment for Autonomous Inland Ships*; Aalto University: Espoo, Finland, 2019; Volume 17.
88. Dargahi, T.; Javadi, H.H.S.; Shafiei, H. Securing Underwater Sensor Networks Against Routing Attacks. *Wirel. Pers. Commun.* **2017**, *96*, 2585–2602. [CrossRef]
89. Alharbi, A. *DBSR: A Depth-Based Secure Routing Protocol for Underwater Sensor Networks*; The Science and Information Organization: West Yorkshire, UK, 2020; Volume 11.
90. Yan, H.; Shi, J.; Cui, J.-H. *DBR: Depth-Based Routing for Underwater Sensor Networks*; The Science and Information Organization: West Yorkshire, UK, 2020.
91. Suratkar, S.; Shah, K.; Sood, A.; Loya, A.; Bisure, D.; Patil, U.; Kazi, F. An Adaptive Honeypot Using Q-Learning with Severity Analyzer. *J. Ambient Intell. Humaniz. Comput.* **2021**, *13*, 4865–4876. [CrossRef]
92. Franco, J.; Aris, A.; Canberk, B.; Uluagac, A.S. A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems. *arXiv* **2021**, arXiv:2108.02287v1. [CrossRef]
93. Huang, L.; Zhu, Q. *Adaptive Honeypot Engagement through Reinforcement Learning of Semi-Markov Decision Processes*; Springer: Berlin/Heidelberg, Germany, 2019. [CrossRef]
94. Mohseni-Bonab, S.M.; Hajebrahimi, A.; Kamwa, I.; Moeini, A. Transmission and Distribution Co-Simulation: A Review and Propositions. *IET Gener. Transm. Distrib.* **2020**, *14*, 4631–4642. [CrossRef]
95. Bhattacharjya, K.; De, D. IoUT: Modelling and Simulation of Edge-Drone-Based Software-Defined Smart Internet of Underwater Things. *Simul. Model. Pract. Theory* **2021**, *109*, 102304. [CrossRef]
96. Nayyar, A.; Balas, V.E. Analysis of simulation tools for underwater sensor networks (UWSNs). In *Lecture Notes in Networks and Systems*; Springer: Berlin/Heidelberg, Germany, 2019; Volume 55, pp. 165–180.
97. Petrioli, C.; Petroccia, R.; Spaccini, D.; Vitaletti, A.; Arzilli, T.; Lamanna, D.; Galizial, A.; Renzi, E. The SUNRISE GATE: Accessing the SUNRISE federation of facilities to test solutions for the Internet of underwater things. In Proceedings of the 2014 Underwater Communications and Networking, UComms 2014, Sestri Levante, Italy, 3–5 September 2014; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2014.
98. Fakhar, F. Investigate Network Simulation Tools in Designing and Managing Intelligent Systems. *J. Indormation Syst. Telecommun.* **2019**, *7*, 278–293.
99. Teixeira, F.B.; Ferreira, B.M.; Moreira, N.; Abreu, N.; Villa, M.; Loureiro, J.P.; Cruz, N.A.; Alves, J.C.; Ricardo, M.; Campos, R. A Novel Simulation Platform for Underwater Data Muling Communications Using Autonomous Underwater Vehicles. *Computers* **2021**, *10*, 119. [CrossRef]
100. Guerra, F.; Casari, P.; Zorzi, M. World Ocean Simulation System (WOSS): A simulation tool for underwater networks with realistic propagation modeling. In Proceedings of the 4th ACM International Workshop on UnderWater Networks, WUWNet ’09, New York, NY, USA, 3 November 2009.

101. Katkar, D.; Ghorpade, D.V. Comparative Study of Network Simulator: NS2 and NS3. 2016. Available online: https://www.semanticscholar.org/paper/Comparative-Study-of-Network-Simulator%3A-NS2-and-NS3-Katkar-Ghorpade/676a95605545f1abf74c321367a99944a06576fb (accessed on 20 November 2022).
102. Gazebo. Available online: https://gazebosim.org/home (accessed on 6 October 2022).
103. Mengacci, R.; Zambella, G.; Grioli, G.; Caporale, D.; Catalano, M.G.; Bicchi, A. An Open-Source ROS-Gazebo Toolbox for Simulating Robots with Compliant Actuators. *Front. Robot AI* **2021**, *8*, 3083. [CrossRef]
104. Bajaj, L.; Takai, M.; Ahuja, R.; Tang, K.; Bagrodia, R.; Gerla, M. *GloMoSim: A Scalable Network Simulation Environment*; Network Simulation Tools: Coimbatore, India, 2002.
105. Idris, S.; Karunathilake, T.; Förster, A. Survey and Comparative Study of LoRa-Enabled Simulators for Internet of Things and Wireless Sensor Networks. *Sensors* **2022**, *22*, 5546. [CrossRef]
106. Comparison of GNS3 vs EVE-NG vs Packet Tracer for Networks Simulation. Available online: https://www.networkstraining.com/gns3-vs-eve-ng-vs-cisco-packet-tracer/ (accessed on 20 November 2022).
107. Chhokra, A.; Barreto, C.; Dubey, A.; Karsai, G.; Koutsoukos, X. *Power-Attack: A Comprehensive Tool-Chain for Modeling and Simulating Attacks in Power Systems*; Association for Computing Machinery (ACM): New York, NY, USA, 2021.
108. Balyk, A.; Karpinski, M.; Naglik, A.; Shangytbayeva, G. Using Graphic Network Simulator 3 for DDoS Attacks Simulation Method of Protection against Traffic Termination in VOIP View Project Using Graphic Network Simulator 3 for Ddos Attacks Simulation. *Int. J. Comput.* **2017**, *16*, 219–225. [CrossRef]
109. Aggarwal, P.; Gonzalez, C.; Dutt, V. HackIt: A real-time simulation tool for studying real-world cyberattacks in the laboratory. In *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*; Springer International Publishing: Berlin/Heidelberg, Germany, 2019; pp. 949–959. ISBN 9783030222772.
110. Aggarwal, P.; Gautam, A.; Agarwal, V.; Gonzalez, C.; Dutt, V. HackIT: A human-in-the-loop simulation tool for realistic cyber deception experiments. In Proceedings of the Advances in Intelligent Systems and Computing; Springer: Berlin/Heidelberg, Germany, 2020; Volume 960, pp. 109–121.
111. MITRE ATT&CK®. Available online: https://attack.mitre.org/ (accessed on 4 October 2022).
112. Welcome to CALDERA's Documentation!—Caldera Documentation. Available online: https://caldera.readthedocs.io/en/latest/ (accessed on 4 October 2022).
113. Simulation Software: Protecting Organisations during the Cyber War. Available online: https://www.information-age.com/simulation-software-cyber-war-123484859/ (accessed on 4 October 2022).
114. Zhao, Y.; Wang, Y.; Zhang, H.; Zhang, C.; Yang, C. *Agent-Based Network Security Simulator Nessi2*; Atlantis Press: Amsterdam, The Netherlands, 2015.
115. Le, T.D.; Anwar, A.; Loke, S.W.; Beuran, R.; Tan, Y. Grid Attacksim: A Cyber Attack Simulation Framework for Smart Grids. *Electronics* **2020**, *9*, 1218. [CrossRef]
116. Foreseeti—Foreseeti. Available online: https://foreseeti.com/ (accessed on 20 November 2022).
117. Red Canary. Available online: https://redcanary.com/blog/comparing-red-team-platforms/ (accessed on 20 November 2022).
118. Release the Monkey! How Infection Monkey Tests Network Security. InsiderPro. Available online: https://www.idginsiderpro.com/article/3519490/release-the-monkey-how-infection-monkey-tests-network-security.html (accessed on 20 November 2022).
119. Bloodhound—A Tool for Exploring Active Directory Domain Security—Latest Hacking News. Cyber Security News, Hacking Tools and Penetration Testing Courses. Available online: https://latesthackingnews.com/2018/09/25/bloodhound-a-tool-for-exploring-active-directory-domain-security/ (accessed on 20 November 2022).
120. Cornejo-Lupa, M.A.; Cardinale, Y.; Ticona-Herrera, R.; Barrios-Aranibar, D.; Andrade, M.; Diaz-Amado, J. Ontoslam: An Ontology for Representing Location and Simultaneous Mapping Information for Autonomous Robots. *Robotics* **2021**, *10*, 125. [CrossRef]
121. Le, T.D.; Anwar, A.; Beuran, R.; Loke, S.W. Smart grid co-simulation tools: Review and cybersecurity case study. In Proceedings of the 7th International Conference on Smart Grid, icSmartGrid 2019, Newcastle, NSW, Australia, 9–11 December 2019; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2019; pp. 39–45.
122. Wu, J.; Yang, Y.; Cheng, X.U.N.; Zuo, H.; Cheng, Z. The development of digital twin technology review. In Proceedings of the 2020 Chinese Automation Congress, CAC 2020, Shanghai, China, 6–8 November 2020; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2020; pp. 4901–4906.
123. Kotis, K.; Katasonov, A. Semantic Interoperability on the Internet of Things: The Semantic Smart Gateway Framework. *Int. J. Distrib. Syst. Technol.* **2013**, *4*, 47–69. [CrossRef]
124. Ahmad, I.; Rahman, T.; Zeb, A.; Khan, I.; Ullah, I.; Hamam, H.; Cheikhrouhou, O. Analysis of Security Attacks and Taxonomy in Underwater Wireless Sensor Networks. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 1444024. [CrossRef]
125. Stavrinos, S.; Kotis, K.; Kalloniatis, C. Towards Semantic Modeling and Simulation of Cybersecurity on the Internet of Underwater Things. *IFIP Adv. Inf. Commun. Technol.* **2022**, *646*, 145–156. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.