A Dynamic Cyber Security Situational Awareness Framework for Healthcare ICT Infrastructures

Shareeful, Islam
School of Computing and Information Science, Anglia Ruskin University,UK, shareeful.islam@aru.ac.uk

Spyridon, Papastergiou
Focal POINT, spyrospapastergiou@gmail.com

Haralambos, Mouratidis
Institute for Analytics and Data Science, School of Computer Science and Electronic Engineering, University of Essex, h.mouratidis@essex.ac.uk

The healthcare sectors have experienced a massive technical evolution over the past decade by integration of medical devices with IT at both physical and cyber level for a critical Health Care Information Infrastructure (HCII). HCII provides huge benefits for the health care service delivery but evolving digital interconnectivity among medical and IT devices has also changed the threat landscape. In particular, systems are now more exposed to the cyber-attacks due to sensitivity and criticality of patient health care information and accessibility of medical devices and this pose any potential disruption of healthcare service delivery. There is a need to enhance security and resilience of HCII. In this paper, we present a Cyber Security Situational Awareness Framework that aims to improve the security and resilience of the overall HCII. The framework aims to develop a novel dynamic Situational Awareness approach on the health care ecosystem. We consider bio inspired Swarm Intelligence and its inherent features with the main principles of the Risk and Privacy assessment and management and Incident handling to ensure security and resilience of healthcare service delivery.

CCS CONCEPTS • Security and privacy • Software and application security • Resilience

Additional Keywords and Phrases: Dynamic Situational Awareness, Health Care Information Infrastructure, Risk Management, Swarm Intelligence

1 Introduction

The healthcare sector has undergone dramatic changes in the past several years, primarily spurred by the adoption of new medical technologies including IoT, Cloud Computing, and Big Data. Beginning with the adoption of electronic health records (EHRs) and continuing into the increased use of medical applications, patient portals, connected healthcare and wearables devices , the healthcare sector has been capitalizing on digital advancements to improve overall patient experiences and service delivery. Health Care Information Infrastructures (HCIIs) are complex due to the increasing interconnection of technology in healthcare between devices at the physical and cyber levels. HCII is also considered as critical and sensitive due to their importance for people's well-being and safety. However, the rapid technical evolution of HCIIs has also changed the threat landscape and producing a wide range of security and privacy challenges and increasing the danger of potential cybersecurity attacks in the healthcare sector. The integrated nature introduces new potential entry points for propagating cyber-attacks and risks in terms of, for example, obsolete security infrastructure or outdated systems, infected devices, lack of appropriate security protocols across organizations. Ponemon institute highlighted that healthcare

organizations are not immune to the same threats facing other industries[1]. The most challenging threats are third-party misuse of patient data, process and system failures and insecure mobile apps. KPMG also states that healthcare industry is behind other industries in protecting its infrastructure and data [2]. Therefore, it constitutes a prime target to adversaries offering them high rewards at low costs. A recent research has shown that the risk of falling prey to data breaches is high, due to password sharing, outdated and unpatched software, or exposed and vulnerable servers [2]. Additionally, HCIIs today are unprotected because they address cybersecurity with individual and isolated products. They need to define a high-level security strategy capable of orchestrating multiple security components to identify system vulnerabilities and sophisticated attacks.

In this context, there is a pressing need for the Health operators to protect their interconnected cyber systems and infrastructures for critical healthcare service delivery. Healthcare stakeholders need new approaches that facilitate their collaboration and promote the security-related information sharing. Additionally, it is also necessary to understand the key assets of the HCII and their impacts of the attacks. An Efficient Situational Awareness approach is necessary to support and facilitate the detection and analysis of cyber-attacks and threats, and to increase knowledge on security and privacy risks. This paper presents an overview of Dynamic Situational Awareness Framework (DSAF) that aims to improve the detection and analysis of cyber-attacks and threats on HCIIs and increase the knowledge on the current cyber security and privacy risks. Additionally, the proposed framework builds risk awareness, within the digital Healthcare ecosystem and among the involved Health operators, to enhance their insight into their Healthcare ICT infrastructures and provides them with capability to react in case of security and privacy breaches. The approach includes Bio-inspired computing , i.e., Swarm Intelligence (SI), to communicate security related information among healthcare entities and uses risk assessment and treatment methodologies for developing the overall situational awareness.

2 RELATED WORKS

There are several works in the literature that focus security issues of HCIIs and medical devices.

2.1 Cyber Threats in Healthcare Sectors

In 2017 the US Food and Drug Administration (FDA) issued a safety recommendation [3] that affected, only in the US, about 65, 000 patients. According to the FDA patients that carry Abbott's implantable cardiac pacemakers should proceed to the nearest clinic in order to update their firmware to “reduce the risk of patient harm due to potential exploitation of cybersecurity vulnerabilities”. In a black box security analysis [4], researchers were able to perform eavesdropping, spoofing and replay attacks against implantable cardiac defibrillators just by reverse engineering the proprietary network protocols used. The researchers were capable of issuing commands to the defibrillator, that were supposedly available only via the short-range protocol, through the long-range one thus extending the attack vector from a few centimetres to up to 5 meters. Finally, in a recent technical report [5] a security analysis on implantable cardiac devices ecosystem revealed over 3700 vulnerabilities. Their findings included easily accessible debug ports, lack of firmware protection techniques, insecure authentication mechanisms during the Over-The-Air (OTA) update process, extended use of unencrypted, hardcoded credentials and sensitive patient data.

2.2 Swarm Intelligence

Swarm Intelligence (SI) is an emerging field of biologically-inspired artificial intelligence which exhibits the collective behaviour of social insect such as bees and ants interacting locally with each other and within the environment to solve a distributed problem [10]. This biologically inspired AI algorithms monitor the behaviour of all swarm members in real time and coordinate with each other for making decision. There are many benefits of using SI due to its inherent nature relating to a large number of active agents who are not only flexible and scalable bur also robust for collectively solving problems. Additionally, agents exhibit randomness that enables the continuous exploration of the alternatives for an optimized solution. Swarm-based algorithms have emerged as a family of nature-inspired, population-based algorithms that are capable of producing low-cost, fast and robust solutions to several complex problems.

There are some unique characteristics of swarms which provide attracts of using it to the various applications [14, 15]:

Autonomy: A swarm consists of cooperating of autonomous individuals. Each individual locally communicates with the neighbors and interacts with the environment without any hierarchical structure.

Solidarity: Swarms generally complete tasks that are impossible to complete by the individuals alone. When a task is completed, each member should autonomously look for a new task and cooperates in solidarity

Awareness: Each member must be aware of its surroundings and abilities.

Resiliency: When an individual member is removed, the remaining members should undertake the unfinished tasks. The swarm is potentially robust to errors in the individuals.

Scalable: The system need to be scalable so that individual can be easily added or removed.

SI is widely used in a number of sectors including financial, voting and cyber security. It facilitates to quickly solve complex problems and reach optimized decisions by converging on solutions that optimize combined knowledge, wisdom, insights, and opinions. Unanimous AI develops a swarm platform that connects human agents globally as an online team to participate any complex decision making process in real time [16]. The platform is successfully used for the predication of game and survey purpose. A general comprehensive swarm framework is presented that combines particle swarms and dynamic agents for the distributed sensing and control system [15]. The framework focuses on the dynamics of swarm as a whole rather than individual agents for the decision making process. It also separates the physical parts and behaviour of the swarm members from their decision making capabilities. The adoption of SI in the security is mainly focuses on the anomaly detection in computer networks. A study considers three SI algorithms, i.e., Colony Optimization (ACO), Particle Swarm Optimization (PSO), and Bee Colony Optimization (BCO) for the anomaly detection [11]. The work introduces SI models into attribute outlier detection to detect anomaly. It considers the fittest agents and random moving agents and obtain superior solutions by changing the searching paths or the positions of agents for an optimized solution. A model is developed to classify cyber-attack by combining Ant Bee Colony (ABC) algorithm with random neural network (RNN)[12]. The work consider ABC to train the RNN and NSL-KDD data sets is used for the attack detection with around 91% accuracy. A self-organized agent swarms (SOMAS) approach is considered to improve the network security based upon desired overall system behaviours [13]. The approach aims for better security management in real time.

2.3 Research Novelty

The existing works highlight the different security and privacy challenges of health care sectors and medical devices. In general, existing approaches are unlikely to effectively detect multi-stage attacks and dynamically re-assess the risks, due to the lack of innovation in capturing and correlating events and associated information. The proposed approach aims for a novel Dynamic Situational Awareness Framework (DSAF) that aims to improve security and resilience of HCIIs. It integrates Bio-inspired computing, i.e., Swarm Intelligence (SI), and related techniques to develop an advanced self-organized networks/system to address security and privacy threats in health care sectors. In particular, the proposed work considers the inherent features of swarm for a sophisticated swarm based system. Unlike the existing works, which are generally considered swarm as a reactive agent, our work considers the dynamics of swarm as a whole for the attack identification and supports risk assessment and management activities.

3 The ProPOSED DYNAMIC SITUATIONAL AWARENESS FRAMEWORK (dsaf)

The proposed DSAF aims to improve the security and resilience of the overall HCIIs. Situational awareness is an effective means for cyber defence and human contributions to the situational awareness is necessary for cyber security [9]. To achieve this, it incorporates novel techniques, mechanisms, and processes for enhancing the secure sharing and storage of all sensitive security and privacy related information in order to protect them from unauthorized deletion, tampering, and revision. In particular, the Security and Privacy layer of the framework will ensure the desired level of protection throughout all the phases and layers of the proposed situational awareness framework. This layer will include capabilities and features to orchestrate and leverage application of innovative privacy mechanisms and maximize achievable levels of confidentiality and data protection compliance within and outside HCIIs. The orchestration approach will enable the application of the most appropriate security and data protection methods depending on the privacy requirements, which

cover a wide range of techniques including anonymization, location privacy, obfuscation, pseudonymization, searchable encryption, multi-party computation and verifiable computation, in order to meet the highly demanding regulatory compliance obligations.

3.1 HealthCare Sector Areas of Consideration

The proposed framework aims is to be inspired by the emergence feature of Swarm Intelligence (SI) in order to make the four distinct circles of consideration act as a sole intelligence. As depicted in Figure 1, the health care ecosystem can be represented as being composed by four circles of consideration that puts the patient in the centre of attention. Security needs to consider form these four circles. An overview of the circles is given below:

The first inner circle, our starting point, includes health components that are very close to the user (e.g. implants, sensors).

The second circle encapsulates the previous one as well as all the medical equipment and devices (e.g. pathology scanners and servers) used in health institutes.

The third circle encloses the two previous ones and incorporates the individual HCIIs.

Finally, the fourth and outer circle contains all the above circles and represents the interdependent HCIIs composing the whole health ecosystem including the supporting Health Care Supply Chain Services (HCSCS).

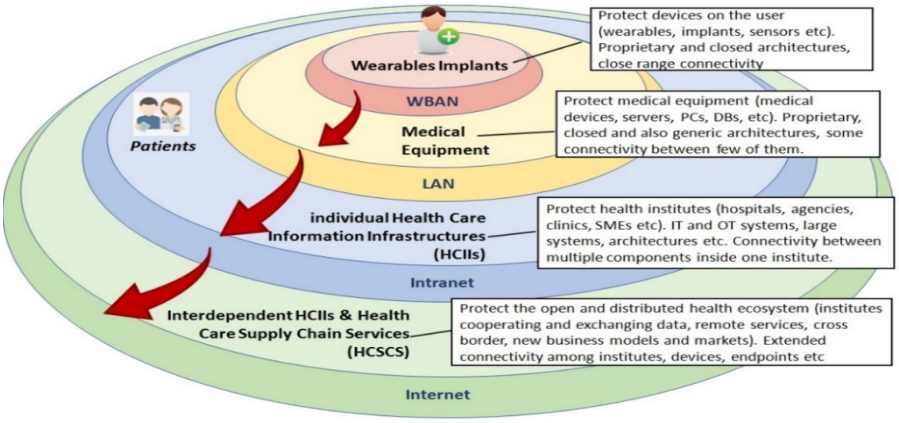

Figure 1: Health Care Circles of Consideration

As presented in Figure 1, each circle area is identified and distinguished based on the homogeneity of characteristics (safety, technical requirements, architectures etc.) identified in each one of them. Table 1 includes the detailed properties of the circle. However, despite the fact that these areas have their own unique characteristics, they are not independent from each other. Inner circles can be seen as the building blocks of the external ones, meaning that the security of the external circles is directly affected by the inner ones. Thus, the security of the interdependent HCIIs and the HCSCS, is directly affected by the security of the individual HCIIs that compose it. However, it should be noted that the overall system is not secured by simply securing its "building blocks". There are interdependences between the different layers that have their own specificities and require cross layer coordination. One example is medical mobile apps (layer: HCSCS) which are connected to user sensors (layer: Wearables) and upload medical data to SMEs' servers (layer: HCIIs).

Table 1: Health Care Circles of Consideration

Circles of Consideration	Criticality of assets	Proximity to user, network range.	Complexity of architectures

Wearables, Implants	Patient health Highest	On or inside user, very short-range networks, WBAN	Devices with closed/proprietary architectures, paired connections
Medical equipment	Patient's health records High	Close or connected to user, local area networks, LAN	Equipment with closed or general architectures, connection between small number of devices
HCIIs	Availability of health services Medium	Close to users or N/A, large area networks, Intranet	Complex IT/OT architectures, management, multiple connections between many devices
Interdependent HCIIs & HCSCS	Community confidence/Reputation Low	N/A, Remote connections, wide area networks, Internet	Dynamic and highly complex health ecosystem. Extended connection between institutes, systems devices etc.

On a scientific level, these four distinct circles of consideration have a complex and interconnected nature that is characterized by the distribution of services, data sharing, the dynamic nature of collaborations and the significant (inter)dependencies among the involved actors, requiring new approaches for the efficient evaluation and treatment of all internal, external and diffused cyber- threats and risks, the estimation of their cascading effects and the thoroughly investigation of a cybersecurity incident (e.g., collection of evidential data). For example, in many cases, the attackers take advantage of the interdependencies in the health care ecosystem, in order to compromise them. Novel multi-stage attacks can be used to exploit vulnerabilities of the interconnected ICT systems to cross the organization's boundaries, enabling the attackers to move within the health ecosystem across multiple critical HCSCS and functions. In this context, because of the number of devices and machines that need to be examined, and the lack of forensic readiness, it's challenging, and at times impossible, to extract and timely and efficient analyses. For example, in HCIIs, the evidential data that should be collected will be from different devices and machines and might be in different formats. Thus, new approaches are required to deal with cascading effects of threats, and propagated vulnerabilities and to react on the security events in their interconnected infrastructures as a sole intelligence.

3.2 Integration of Swarm Intelligence

The proposed approach is inspired by the emergence feature of Swarm Intelligence (SI) in order to make the four distinct circles of consideration act as a sole intelligence. The idea of SI is based on the organizational format observed in natural communities, where individual members perform very simple actions co-operating with one another. These actions gradually accumulate, to form a higher-level intelligence which does not exist in any of the individual members contributing to it. An indicative example of the SI logic is ant colonies, whose members co-operate with one another coordinated through a chemical substance called pheromone, gradually achieving to find the optimal path towards resources, a process perfected in the course of thousands of years of evolution. Interdependent infrastructures can also use new advanced approaches to play the part that evolution has played for insects. The framework intends to transfer the emergence idea of SI, enabling the creation of an underlying autonomous computing infrastructure technology in a way it had never been done before. More specifically, biological principles (i.e., Bio-inspired computing) will be applied to the design of advanced self-organized networks/systems, combining knowledge from the fields of biology, computer science and mathematics. Basic principles on their design include the decentralized exchange of knowledge and the support of self-functionalities in the network (e.g., self-organization, self-awareness). Through the research to be conducted, the homogeneous nodes will be enabled to act in a swarm-based manner, to detect, analyse and mitigate security and privacy risks, ongoing attacks and threats, security incidents and privacy breaches, and eventually to establish risk awareness [7].

To this end, the framework vision is to introduce a novel Situational Awareness approach on the health care ecosystem, which combines the shared features of SI with the main principles of the Risk and Privacy assessment and management approaches, towards strengthening the security, resilience and robustness of the interconnected HCIIs. The proposed framework will seek to develop new types of management and coordination schemes and structures. These schemas will be able to adapt their functionality to the decisions and targets that the HCIIs will set, thus acting as facilitators that will

enable them to self-organize, and at the same time they will exhibit the emergent behaviour that has so much proven to benefit swarm communities. This is needed to identify and harness the information and knowledge that the individual HCIIs' nodes have about the cyber-risks, threats and cyber-attacks in timely and cost-effective manner, and coordinate them in a self-regulating manner to elevate their intelligence. The concept of self-organization of the framework will provide reliability, robustness, energy efficiency and scalability in the project's cybersecurity and privacy risk and incident awareness mechanisms.

3.3 Principles

The main goal of the proposed approach is to improve, intensify and coordinate the overall security efforts for the effective and efficient identification, evaluation, investigation and mitigation of realistic risks, threats and multi-dimensional attacks within the cyber assets in the four distinct areas of consideration as shown in Figure 2. The proposed approach seeks to support, prepare and help the Interdependent HCIIs participating in different types of HCSCS to:

thoroughly assess the vulnerabilities of all cyber assets;
continuously forecast and evaluate the probability of cyber-attacks;
access/receive warnings for upcoming attacks and vulnerabilities;
easily recreate, visualize and forecast propagation and cascading effects of attacks in their Interdependent HCIIs and anticipate how these attacks propagate across the HCSCS;

Figure 2 presents the main aspects and principles of DSA, which is built upon a new type of SI, self-organizing and dynamic collaboration approach implemented through an individualised Autonomous Networking protocol that provides autonomic deployment, cluster formulation and hierarchical communication in HCIIs. This protocol, will connect the four circles of the health ecosystem grouping individual ICT elements, systems and components into a population of simple or group of nodes, named AICS nodes (group of ICT assets or individual HCIIs), allowing them to interact locally with one another and with their Interdependent Health Care environment. The interaction is considers using a number of agents who are linked together and cooperate with each other through local interactions to achieve distributed optimization of the risk analysis and incident handling in real time. The continuous diffusion of security-related information across the network enables the agents to optimize the evaluation and mitigation of the interdependent threats and risks as well the investigation of complex security events and data breaches.

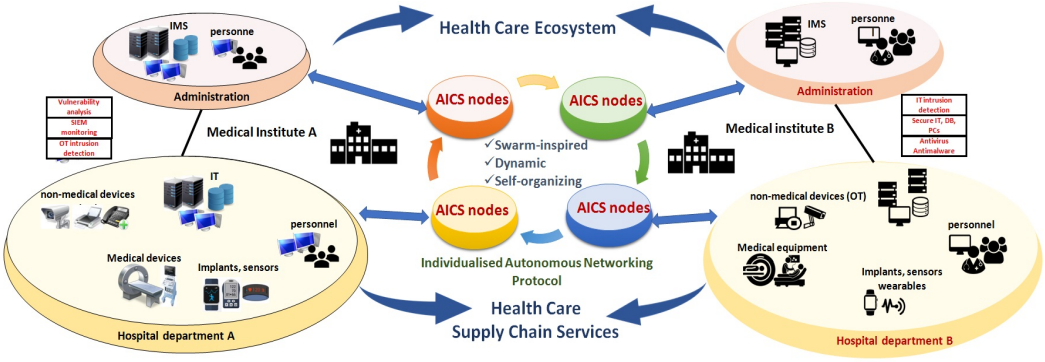

Figure 2: Main Aspects and Principles of DSAF

The DSAF relies on the following principles:

Swarm-inspired: All AICS nodes of the Interdependent HCIIs will perform only a specific set of simple individual actions, including: (a) evaluation of risk and privacy risk; (b) identification of propagated vulnerabilities located in interconnected infrastructures; (c) estimation of the cascading effects of threats or detected events; (d) detection of security incidents; (e) uncovering evidence of malicious activities; (f) extraction and collection of data of particular interest; (g) analysing and correlating relationships between all recovered forensic artefacts;

(h) anticipation of where an attack is heading; (i) provision of recommendations, advices and directions on the further investigation of the security incident; and (j) proposal of a mitigation/containment strategy.

Dynamic: The AICS nodes of the Interdependent HCIIs do not have to possess global knowledge over all the actions that other entities perform, nor do they have to keep up with all the information and knowledge exchanges that take place inside the system. They act locally; performing their own actions, which however if accumulated, provide the healthcare ecosystem with the potential of assessing and handling risk, threats and incidents effectively. In this context, the nodes share only the security-related information required from the other nodes to further estimate the risk and investigate an event.

Self-organizing: Coordination of the AICS nodes towards analysing security and privacy risks and events providing implicit guidance. In other words, all the decisions should be indicated by the aggregated activities of the individual nodes. Such activities include notifying the appropriate node that each time should be mobilized to participate in the risk evaluation and investigation process.

4 Conclusions

Cyber-attack is constantly increasing for the Health Care Information Infrastructure (HCII). There is a need to develop innovative solutions for improving security and resilience of the HCII. This paper provides an overview of a dynamic self-organized SI Situational Awareness Approach that improves the detection and analysis of cyber-attacks and threats on HCIIs and increases the knowledge on cyber security and privacy risks. The framework adopts the dynamic behaviour of self-organized swarm for cyber-attack analysis and risk management. Such self-organized system consists typically of a population of simple or group of nodes (group of ICT assets or individual entities), interacting locally with one another and with their HC environment for tackling the risks. As future work, we are planning to include suitable swarm intelligence algorithm and underlying communication protocol for the framework. Additionally, it is also necessary to evaluate the framework through use cases targeting for medical implant and Personal Health Systems with On-Body-Sensors/Actors.

ACKNOWLEDGMENTS

This work was partially supported by the AI4HEALTHSEC EU project, funded from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273

REFERENCES

<bib id="bib1"><number>[1]</number>Ponemon Institute (2018), The State of Cybersecurity in Healthcare Organizations in 2018, https://ponemonsullivanreport com/2018/03/the-state-of-cybersecurity-in-healthcare-organizations-in-2018/</bib>
<bib id="bib2"><number>[2]</number>KPMG (2015), Health Care and Cyber Security, Increasing Threats Require Increased Capabilities</bib>
<bib id="bib3"><number>[3]</number>Smith, D., In Review: Healthcare Under Attack, 2018, https://blog.radware.com/security/applicationsecurity/2018/12/2018-in-review-healthcare-under-attack/</bib>
<bib id="bib4"><number>[4]</number>https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals</bib>
<bib id="bib5"><number>[5]</number>Marin, E., Singelée,D., Garcia, F., Chothia, T., Willems, R., Preneel, B. , (2016) On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them, In Proceedings of the 32nd Annual Conference on Computer Security Applications December 2016 Pages 226–236https://doi.org/10.1145/2991079.2991094</bib>
<bib id="bib6"><number>[6]</number>Rios, B., Butts, J., Security Evaluation of the Implantable Cardiac Device Ecosystem Architecture and Implementation Interdependencies,2017 , https://www.ledecodeur.ch/wp-content/uploads/2017/05/Pacemaker-Ecosystem-Evaluation.pdf</bib>
<bib id="bib7"><number>[7]</number>ISE Report on Securing Hospitals, https://securityevaluators.com/hospitalhack/ </bib>
<bib id="bib8"><number>[8]</number>S.-Y. Tu and A. H. Sayed, "Distributed decision-making over adaptive networks, " IEEE Trans. Signal Processing, March 2014.</bib>
<bib id="bib9"><number>[9]</number>Tyworth et al 2013, Tyworth, M., Giacobe N., Mancuso V. , McNeese M. , Hall, L. D., Human-In-The-Loop Approach to Understanding Situation Awareness in Cyber Defense Analysis. EAI Endorsed Transactions on Security and Safety 2013.</bib>
<bib id="bib10"><number>[10]</number>Ahmed, H., Glasgow, J.(2012). Swarm Intelligence: Concepts, Models and Applications, Technical Report 2012-585, School of Computing Queen's University.</bib>
<bib id="bib11"><number>[11]</number>Bo Liu, Mei Cai and Jiazong Yu , Swarm Intelligence and its Application in Abnormal Data Detection, Informatica , Vol 39(1), 2015</bib>
<bib id="bib12"><number>[12]</number>Ayyaz-Ul-Haq Qureshi, Hadi Larijani, Abbas Javed, Nhamoinesu Mtetwa, Jawad Ahmad, Intrusion Detection Using Swarm Intelligence, China Emerging Technologies (UCET) ,2019</bib>
<bib id="bib13"><number>[13]</number>Eric M. Holloway and Gary B. Lamont and Gilbert L. Peterson , Network Security Using Self Organized Multi Agent Swarms, IEEE Symposium on Computational Intelligence in Cyber Security,2009 </bib>
<bib id="bib14"><number>[14]</number>J. Kennedy and R. C. Eberhart, Swarm Intelligence. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2001.</bib>

<bib id="bib15"><number>[15]</number>Jelmer van Ast; Robert Babuska; Bart De Schutter , A general modeling framework for swarms, 2008 IEEE Congress on Evolutionary Computation (IEEE World Congress on Computational Intelligence)</bib>
<bib id="bib16"><number>[16]</number>L. Rosenberg, G. Willcox, Artificial Swarm Intelligence, Unanimous AI</bib>