Human Factors in Cybersecurity, Vol. 127, 2024, 208–218
https://doi.org/10.54941/ahfe1004780

A Self-Organized Swarm Intelligence Solution for Healthcare ICT Security

Kitty Kioskli[1,2], Spyridon Papastergiou[2], Theofanis Fotis[3,4], Stefano Silvestri[5], and Haralambos Mouratidis[1]

[1]University of Essex, School of Computer Science and Electronic Engineering, Institute of Analytics and Data Science (IADS), Parkside Office Village, Wivenhoe Park, Colchester CO4 3SQ, United Kingdom
[2]University of Piraeus, Department of Informatics, Piraeus, Greece
[3]trustilio B.V., Vijzelstraat 68, 1017 HL Amsterdam, The Netherlands
[4]University of Brighton, School of Health Sciences, Centre for Secure, Intelligent and Usable Systems (CSIUS), Brighton, BN1 9PH, United Kingdom
[5]Institute for High Performance Computing and Networking of the National Research Council of Italy Via Pietro Castellino, 111 - 80131, Naples, Italy

ABSTRACT

The healthcare sector has undergone a transformative evolution through the integration of advanced technologies such as IoT, Cloud Computing, and Big Data. This progression, starting with electronic health records, now includes a diverse array of digital tools, from medical apps to wearables. These innovations have significantly improved patient experiences and outcomes, forming extensive Health Care Information Infrastructures (HCIIs). Consequently, the security of interdependent HCIIs and Health Care Supply Chain (HCSCS) is intrinsically linked to the security of each individual HCIIs that constitute the collective network. Currently, HCIIs face vulnerabilities due to reliance on isolated cybersecurity products, necessitating a unified security strategy. Recognizing the criticality of assets, prioritizing emerging solutions becomes crucial to mitigating complexity. The evolving landscape of cyber threats in healthcare demands collaboration among European health and cybersecurity experts to establish policies and standards, elevating security maturity across the EU. The proposed solution in this study represents a cutting-edge approach to healthcare cybersecurity. It enhances threat detection, analysis, and privacy awareness in the digital healthcare ecosystem through a Dynamic Situational Awareness Framework. This empowers stakeholders to recognize and respond to cyber risks effectively, including advanced persistent threats and daily incidents. The solution facilitates secure incident-related information exchange, strengthening the security and resilience of modern digital healthcare systems and supply chain services. The innovative approach draws inspiration from biological swarm formations, integrating security engineering, privacy engineering, and artificial intelligence. By creating a highly interconnected intelligence system, it enables local interactions and management in healthcare environments. Employing bio-inspired techniques and large-group decision-making models enhances communication and coordination in complex, distributed networks. The framework prioritizes scalability and fault-tolerance, streamlining investigation activities and fostering dynamic intelligence and collective decision-making within healthcare ecosystems.

Keywords: Healthcare cybersecurity, Framework, Swarm intelligence, Human systems integration

INTRODUCTION

The healthcare sector has undergone significant changes, driven by the adoption of new technologies like IoT, Cloud Computing, and Big Data. From electronic health records (EHRs) to medical apps, patient portals, and wearables, digital advancements aim to improve patient experiences. The increasing integration of technology has transformed healthcare into large Health Care Information Infrastructures (HCIIs), critical for well-being and safety. Direct actions, like inadequate medical care or disabling devices, pose risks. Indirect actions, such as altering records or disrupting operations, can have severe consequences. Safeguarding these systems is crucial for patient safety in the evolving digital healthcare landscape.

The evolving digital interconnectivity of medical devices has transformed the threat landscape. The digitization of patient data is now a prime target for cybercriminals, resulting in a myriad of security and privacy challenges and an increased risk of cybersecurity attacks in HCIIs. From a cyber-physical perspective, the stakes involve not just information but also other cyber and kinetic assets. Given the sensitivity and confidentiality of health data, information security becomes a critical concern. Health critical infrastructures, with cyber-physical aspects like remotely controlled medical equipment, pose potential risks of causing patient harm. Hospitals, health plans, and research labs manage unique and valuable assets increasingly exposed to cyber threats. Personal health information (PHI) and electronic health records (EHRs) constitute highly sensitive assets unique to healthcare infrastructures. According to the Ponemon Institute, "healthcare organizations are not immune to the same threats facing other industries." The most challenging threats include cyber-attacks, third-party misuse of patient data, process and system failures, and insecure mobile apps. The allure for adversaries lies in the high value of healthcare assets and the relative ease with which they can be compromised. KPMG highlights that the healthcare industry lags behind other sectors in protecting its infrastructure and data. Consequently, it becomes a prime target for adversaries seeking high rewards at low costs.

A recent study (Islam et al., 2021) has highlighted that the risk of falling victim to data breaches is substantial, primarily due to factors such as password sharing, outdated and unpatched software, and exposed and vulnerable servers. Additionally, significant cyberattacks and vulnerabilities have been identified in near-patient healthcare devices. In 2017, the US Food and Drug Administration (FDA) issued a safety recommendation [4] affecting approximately 65,000 patients in the US alone. The FDA advised patients with Abbott's implantable cardiac pacemakers to visit the nearest clinic for a firmware update, aiming to "reduce the risk of patient harm due to potential exploitation of cybersecurity vulnerabilities." In a black box security analysis, researchers demonstrated eavesdropping, spoofing, and replay attacks on implantable cardiac defibrillators by reverse engineering proprietary network protocols. The researchers could issue commands to the defibrillator, originally accessible only via short-range protocol, through the long-range protocol, extending the attack vector from a few centimetres to up to 5 meters. In a recent technical report (Rios & Butts, 2017), a security analysis

of the implantable cardiac devices ecosystem revealed over 3700 vulnerabilities. Findings included easily accessible debug ports, a lack of firmware protection techniques, insecure authentication mechanisms during Over-The-Air (OTA) updates, widespread use of unencrypted, hardcoded credentials, and the exposure of sensitive patient data.

In this context, there is a critical imperative for healthcare operators to safeguard their interconnected cyber systems and infrastructures. Efficient situational awareness approaches (i.e., threat intelligence platforms, security information and event management systems) are essential to detect and analyze cyber-attacks and threats, as well as to enhance understanding of security and privacy risks. To assess cyber risks in the health sector, it is vital to comprehend the systems to be defended, their key assets, and the impacts of potential attacks. Furthermore, identifying and analyzing potential adversaries is equally crucial. Existing approaches often fall short in effectively detecting multi-stage attacks and dynamically reassessing risks, mainly due to a lack of innovation in capturing and correlating events and associated information.

This paper proposes a state-of-the-art solution aimed at improving the detection and analysis of cyber-attacks and threats on HCIIs, elevating awareness of current cybersecurity and privacy risks. The solution also cultivates risk awareness within the digital healthcare ecosystem and among healthcare operators, providing them with the capability to respond in the event of security and privacy breaches. Importantly, this solution promotes the exchange of reliable and trusted incident-related information among ICT systems and entities comprising HCIIs, all without revealing sensitive corporate details.

OVERALL CONCEPT

In the digital era, the healthcare ecosystem in Europe has evolved into a complex mosaic, comprising large health systems, institutes, single physician practices, SMEs, research labs, device developers, and more. This ecosystem is best described as a widely distributed, interconnected set of entities (organizations, individuals, and/or critical infrastructures), processes, and services that rely on interconnected ICT infrastructures, forming a dynamic Health Care Supply Chain (HCSC). The established interconnections reflect the relationships among the involved entities. Within this context, HCSCs exhibit a high degree of complexity and interconnectivity in their ICT systems. As illustrated in Figure 1, the healthcare ecosystem can be depicted as consisting of four concentric circles, with the patient at the center. The first inner circle, our starting point, includes health components closely linked to the user (e.g., implants, sensors). The second circle encompasses the previous one and includes all medical equipment and devices (e.g., pathology scanners and servers) used in health institutes. The third circle encompasses the two previous circles and incorporates individual Health Care Information Infrastructures (HCIIs). Finally, the fourth and outermost circle comprises all the preceding circles, representing the interdependent HCIIs that constitute the entire health ecosystem, including the supporting Health Care Supply Chain Services (HCSCS). These four circles, detailed in Table 1, were identified and

distinguished based on the homogeneity of characteristics (safety, technical requirements, architectures, etc.) identified in each of them.

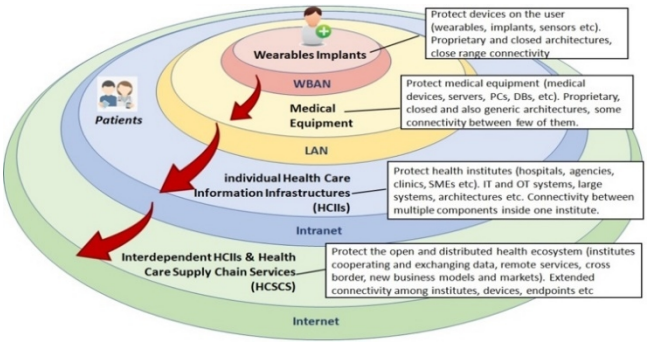

Figure 1: Solution's circles of consideration.

As previously highlighted, there is an urgent imperative to ensure the proper security of the identified four distinct areas of consideration. Despite each area having its unique characteristics, they are interconnected; the inner circles can be viewed as the building blocks of the external ones. This implies that the security of the external circles is directly influenced by the security of the inner ones. Therefore, the security of the interdependent HCIIs and the HCSCS is directly impacted by the security of the individual HCIIs comprising it. However, securing the "building blocks" alone does not guarantee the overall system's security. There are interdependencies between the different layers, each with its specificities, necessitating cross-layer coordination. A prime example is medical mobile apps (layer: HCSCS) connected to (or using their own) user sensors (layer: Wearables) and uploading medical data to SMEs' servers (layer: HCIIs).

Table 1. Analysis of circles of consideration.

Circles of Consideration	Criticality of Assets	Proximity to User, Network Range	Complexity of Architecture
Wearables, Implants	Patient Health Highest	On or inside user, very strange-range Networks, WBAN	Devices with closed architectures, paired connections
Medical Equipment	Patients' 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 user 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

From a scientific perspective, these four distinct circles of consideration possess a complex and interconnected nature characterized by the distribution of services, data sharing, dynamic collaborations, and significant (inter) dependencies among the involved actors. This complexity necessitates innovative approaches for the efficient evaluation and treatment of all internal, external, and diffused cyber threats and risks. It also involves estimating cascading effects and thoroughly investigating cybersecurity incidents, including the collection of evidential data. For instance, attackers often exploit interdependencies in the healthcare ecosystem to compromise it. Novel multi-stage attacks may exploit vulnerabilities in interconnected ICT systems, crossing organizational boundaries and enabling attackers to traverse the health ecosystem through multiple critical Health Care Supply Chain Services (HCSCS) and functions. Given the multitude of devices and machines that need examination and the lack of forensic readiness, extracting and analyzing evidential data in a timely and efficient manner is challenging and sometimes impossible. In HCIIs, evidential data must be collected from different devices and machines, potentially in various formats. Consequently, new approaches are required to address cascading effects of threats, propagated vulnerabilities, and to respond to security events within interconnected infrastructures as a unified intelligence.

Our proposed solution aims to harness the emergent features of Swarm Intelligence (SI) to unify the four distinct circles of consideration into a cohesive intelligence. The concept of SI is drawn from the organizational format observed in natural communities, where individual members perform simple actions in cooperation. These actions gradually accumulate to form a higher-level intelligence that doesn't exist in any of the individual members contributing to it. Ant colonies serve as an indicative example of SI logic, where members cooperate through a chemical substance called pheromone to find the optimal path towards resources, a process perfected over thousands of years of evolution. Interdependent infrastructures can similarly adopt advanced approaches to mimic the evolutionary benefits seen in insects. This solution will transfer the emergence idea of SI, creating an underlying autonomous computing infrastructure technology in a ground breaking manner. Specifically, we will apply principles from bio-inspired computing to design advanced self-organized networks/systems, drawing on knowledge from biology, computer science, and mathematics. Key design principles include the decentralized exchange of knowledge and the support of self-functionalities in the network, such as self-organization and self-awareness. Through our research, homogeneous nodes will act in a swarm-based manner to detect, analyze, and mitigate security and privacy risks, ongoing attacks and threats, security incidents, and privacy breaches, ultimately establishing risk awareness (Tu & Sayed, 2014). Our proposed solution envisions introducing a novel Situational Awareness approach to the healthcare ecosystem, combining the shared features of SI with the main principles of risk and privacy assessment and management approaches, as well as incident handling models. This vision aims to strengthen the security, resilience, and robustness of interconnected HCIIs, along with supporting medical supply chain services and functions, utilizing all available threat intelligence information.

METHODOLOGY

The primary outcome of the solution is the development of the Artificial Intelligence Dynamic Situational Awareness Framework (DSAF). The proposed approach aims to enhance overall security efforts by effectively identifying, evaluating, investigating, and mitigating realistic risks, threats, and multidimensional attacks within the cyber assets of the four distinct areas of consideration (Figure 1). The approach supports Interdependent HCIIs in various Health Care Supply Chain Services (HCSCS) by thoroughly assessing vulnerabilities, continuously forecasting and evaluating the probability of cyber-attacks, providing warnings for upcoming threats, understanding the continuum of cybersecurity indicators, visualizing and forecasting attack propagation, and offering a targeted step-by-step framework for investigating and handling complex incidents. Additionally, it facilitates the extraction, combination, and analysis of security incident-related information, offering guidelines and enabling the sharing of information and warnings among all HCIIs.

For the proposed framework to achieve its objectives, the DSAF (Figure 2) will be constructed based on a new type of SI incorporating a self-organizing and dynamic collaboration approach. This will be implemented through an individualized Autonomous Networking protocol that provides autonomic deployment, cluster formulation, and hierarchical communication within HCIIs. The protocol will interconnect the four circles of the health ecosystem, grouping individual ICT elements, systems, and components into a population of nodes known as AICS nodes (group of ICT assets or individual HCIIs). This enables local interactions among nodes and with their Interdependent Health Care environment. The protocol establishes networking infrastructures, as depicted in Vertical Layer 1 – Information Sharing & Individualized Autonomous Networking of the DSAF, to effectively coordinate AICS nodes of Interdependent HCIIs by defining and leveraging actions to be performed. These agents collaborate through local interactions for distributed optimization of real-time risk analysis and incident handling. Continuous diffusion of security-related information across the network facilitates optimized evaluation and mitigation of interdependent threats and risks, as well as the investigation of complex security events and data breaches.

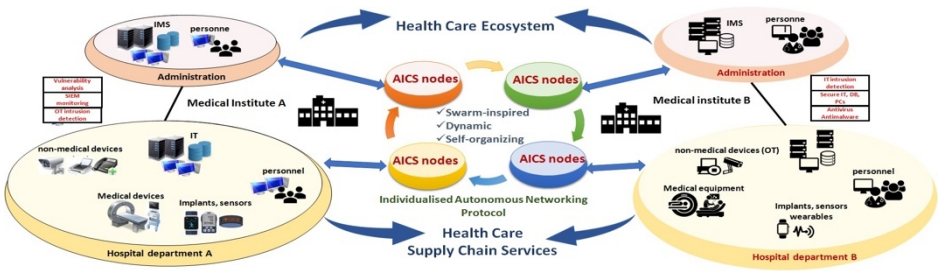

Figure 2: Main aspects and principles of the framework.

It's noteworthy that the solution will leverage existing diffusion strategies for adaptation and information sharing, including adaptive diffusion strategies and steepest-descent diffusion strategies. Additionally, the DSAF relies on the following principles:

- **Swarm-inspired**: All AICS nodes within Interdependent HCIIs perform specific sets of simple individual actions, including the evaluation of risk and privacy risk, identification of propagated vulnerabilities in interconnected infrastructures, estimation of the cascading effects of threats or detected events, detection of security incidents, uncovering evidence of malicious activities, extraction and collection of data of particular interest, analysis and correlation of relationships between all recovered forensic artifacts, anticipation of the direction of an attack, provision of recommendations, advice, and directions for further investigation of security incidents, and proposal of a mitigation strategy.
- **Dynamic**: AICS nodes of Interdependent HCIIs do not require global knowledge of all actions performed by other entities, nor do they need to keep up with all information and knowledge exchanges within the system. They act locally, performing their own actions, which, when accumulated, provide the healthcare ecosystem with the potential to assess and handle risks, threats, and incidents effectively. In this context, nodes share only the security-related information required from other nodes to estimate risk and investigate an event.
- **Self-organizing:** Coordination of AICS nodes towards analyzing security and privacy risks and events provides implicit guidance. In other words, decisions are indicated by the aggregated activities of individual nodes, including notifying the appropriate node each time it should be mobilized to participate in the risk evaluation and investigation process.

CONCEPTUAL DYNAMIC SITUATIONAL AWARENESS FRAMEWORK

The goal of the DSAF is to assess security and privacy risks, detect new, sophisticated, and persistent threats, handle complex cybersecurity incidents and data breaches, and share all individual risks, threats, and incident-related information while ensuring their integrity and validity. This is achieved through the incorporation of a set of well-defined data mining, Global Artificial Intelligence, and machine learning techniques and models. The proposed approach addresses both technical and cognitive challenges. From a technical perspective, the model focuses on collecting, compiling, processing, and fusing all individual security-related information, ensuring their integrity and validity. In contrast, from a cognitive point of view, decision-makers should understand the technical aspects of risks, threats, and attacks and draw conclusions on how to respond.

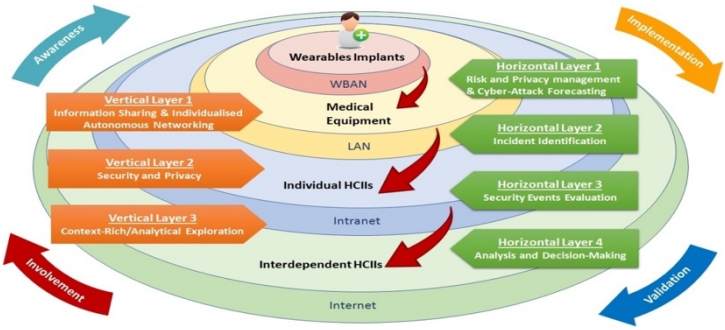

Figure 3: Framework overview.

The proposed framework (Figure 3) comprises four main phases:

(a) **Awareness & Recommendations Phase:** This phase is characterized by proactiveness, and AICS nodes of the Interdependent HCIIs should be in a state of readiness to achieve the required awareness level. It involves the identification and modeling of goals and network environment, security awareness requirements, as well as legal/forensic, security, and privacy requirements. This phase leads to the creation of recommendations and security plans for designing solutions and security services to protect each individual node independently. The combination of these data results in the initial definition of security systems for each AICS node and the identification of any missing competences and tools. This phase includes the following activities:

Organizational modeling: AI4HEALTHSEC adopts a bottom-up approach, identifying the goals of each AICS node along with its ICT assets, their relationships, and interdependencies with other entities.

Security, privacy, and incident handling requirements modeling: Conceptually integrating security and privacy management, risk assessment, and incident handling requirements into every relevant phase of the situational awareness process. Goal-oriented modeling approaches are employed, considering international and local legislation in incident handling design due to potential variations in evidence requirements.

Intelligence model instantiation: This involves instantiating the intelligence model, capturing the right data for timely risk evaluation and incident detection. Data can originate from security systems, software, vulnerability repositories, threat sharing schemes, etc. Dynamic intelligence requires techniques to describe security intelligence from a system's perspective, identifying and modeling information to be exchanged between AICS nodes, its usage, and how this information combines with other data to form intelligence.

(b) **Implementation Phase:** This phase encompasses the full steps of a comprehensive cybersecurity situational awareness lifecycle, incorporating procedures for risk assessment, vulnerability detection, and incident handling. Figure 3 illustrates the overall structure of this phase, consisting of 7 main conceptual layers: 4 horizontal layers dealing with the situational

awareness process and three vertical layers, including "Information Sharing & Individualized Autonomous Networking," responsible for distributing, disseminating, self-publishing, broadcasting, or circulating security-related information; "Security & Privacy," incorporating security, privacy, and data protection features; and "Context-Rich/Analytical Exploration," providing an analytical approach to risk and incident characteristics based on a predefined set of key performance indicators (KPIs), facts, and dimensions. These layers serve as the conceptual pillars for building and implementing the solution's components that support the modeling, evaluation, and investigation of various cybersecurity-related risks, threats, and incidents.

It's important to note that this phase also involves the development of focused solutions for each layer. These solutions, built and validated based on existing technologies with a medium Technology Readiness Level (TRL) contributed by project partners, take advantage of their existing related technologies. High-quality research innovations and state-of-the-art products in the areas of cyber-protection are appropriately adapted and enhanced with a set of well-defined data mining, Global Artificial Intelligence, and machine learning techniques and models. The aim is to provide a motivating and user-friendly system, empowering HCIIs to collaboratively assess, model, anticipate, treat, and predict multidimensional risks, threats, and attacks.

(c) **Validation Phase:** In this phase, our solution strategically selects four distinct pilots to evaluate proposed solutions across vertical and horizontal contexts. This approach enables the consortium to gather requirements from diverse inputs, explore multiple aspects of the problem, address cross-layer, cross-technology, and cross-domain use cases, and delve into crucial development issues such as performance, flexibility, reusability, common solutions versus specific use cases, and more.

(d) **Involvement Phase:** The final phase integrates input from all preceding phases to develop comprehensive training courses aimed at involving users in "security and privacy thinking and doing." Additionally, a dedicated website will be established, linked with other training platforms used in the project, to host information and materials (security tools, recommendations, reports, etc.) generated within and outside the solution's context for health cybersecurity. This website serves as a hub of interest for stakeholders, and efforts to attract and engage individuals through features like forums will be explored and developed throughout the project's duration.

CONCLUSION

In conclusion, the proposed Artificial Intelligence DSAF for health cybersecurity represents a comprehensive and innovative approach to addressing the complex challenges faced by Interdependent HCIIs. Leveraging principles of SI and advanced autonomous networking protocols, the DSAF aims to unify disparate elements within the health ecosystem, enhancing overall security efforts. The framework's multi-phase implementation encompasses proactive awareness and recommendation stages, dynamic and self-organizing Swarm-inspired execution, and a thorough validation process through real-world pilots. Importantly, the involvement phase ensures that the solution is not

only technically robust but also user-friendly, promoting a broader understanding of security and privacy considerations within healthcare settings. Through the careful consideration of technical and cognitive challenges, the DSAF integrates data mining, Global Artificial Intelligence, and machine learning techniques to evaluate security and privacy risks, detect threats, and handle complex incidents. The framework's emphasis on individualized autonomous networking, information sharing, and analytical exploration enriches the overall cybersecurity situational awareness lifecycle. The validation phase, involving diverse pilot contexts, ensures adaptability and performance across various scenarios. The commitment to user involvement and training courses, coupled with the creation of a dedicated website for information dissemination, highlights a holistic approach to fostering stakeholder engagement and knowledge-sharing within the healthcare cybersecurity domain. Ultimately, the proposed DSAF emerges as a promising solution, poised to strengthen the resilience, security, and collaborative capabilities of healthcare information infrastructures in the face of evolving cyber threats.

ACKNOWLEDGMENT

The research conducted in this paper was funded by the project: 'A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures' (AI4HEALTHSEC) under grant agreement (GA) No 883273. The project was funded by the European Union's Horizon 2020 research and innovation programme; 'Collaborative, Multi- modal and Agile Professional Cybersecurity Training Program for a Skilled Workforce In the European Digital Single Market and Industries' (CyberSecPro) project, which has received funding from the European Union's Digital Europe Programme (DEP) programme under GA No 101083594; 'Human-centered Trustworthiness Optimisation in Hybrid Decision Support' (THEMIS 5.0) project, which has received funding from the European Union's Horizon Programme under GA No 101121042; 'advaNced cybErsecurity awaReness ecOsystem for SMEs' (NERO) project, which has received funding from the European Union's DEP programme under GA No 101127411;'Fostering Artificial Intelligence Trust for Humans towards the optimization of trustworthiness through large-scale pilots in critical domains' (FAITH) project, which has received funding from the European Union's Horizon Programme under GA No 101135932. The views expressed in this paper represent only the views of the authors.

REFERENCES

https://blog.radware.com/security/applicationsecurity/2018/12/2018-in-review-healthcare-under-attack/

https://www.esat.kuleuven.be/cosic/publications/article-2678.pdf

https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals

KPMG (2015), Health Care and Cyber Security: Increasing Threats Require Increased Capabilities

Ponemon Institute (2018), The State of Cybersecurity in Healthcare Organizations in 2018 .

S.-Y. Tu and A. H. Sayed (2014), "Distributed decision-making over adaptive networks," IEEE Trans. Signal Processing.