IoT vulnerabilities in military environments

Abstract

IoT devices (sensors, drones, cameras) are gaining more and more emphasis on military operations. The application of IoT elements in the military environment increases situational awareness and supports the acquisition and maintenance of information superiority. The information they provide about the enemy, the area of operations, and the location and status of our soldiers and assets can contribute to the successful execution of operations at the tactical, operational and strategic levels. However, they can also pose serious threats if their vulnerabilities allow the data they collected to leak or they provide access to the info-communication networks used for the enemy. In this article, the author examined the vulnerabilities of these IoT devices using keyword analysis. After drawing conclusions from the analysis of the relevant literature, he compared the results with the general-purpose IoT threats and attacks typical of today, like distributed denial of service attacks, security, software, security and privacy issues.

Keywords: IoT vulnerabilities, Military Internet of Things, Internet of Battlefield Things, DDoS, privacy protection

Introduction

The Internet of Things is a communication paradigm that aims to connect different devices to the Internet (networks) to collect data gathered by sensors, provide remote control of devices and systems, and continuously monitor the environment, the vehicles, the devices, and people.[1] IoT devices are very widespread and used nowadays. A Juniper report states that the number of IoT devices is expected to reach 83 billion by 2024; with most new items appearing in the industrial and agricultural environment, more than 70% of IoT connections will be deployed in this environment.[2] They have also appeared in military operations in recent years and are becoming increasingly important in successful operations in modern warfare. Accordingly, more and more new concepts are emerging, such as military IoT (MIoT), Internet of Battlefield Things (IoBT), and Internet of Flying Things (IoFT). These terms appear mostly in military literature, as they are used in operational environments. IoT devices used in the military environment primarily support Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems to provide situational awareness to commanders and staffs. An adaptation of the IoT to the military domain is the Military Internet of Things, which focused on the connectivity of military objects/devices that can communicate without human intervention. The IoT is a set of devices and components used for military purposes with the primary goal of data collection, automation and remote control. Accordingly, IoT devices used in a military environment may be vehicles, instruments, weapon systems or parts thereof, medical/health devices, electrical networks, transport infrastructures, building systems, or even nodes with sensing and transmission capabilities.[3] Using IoT devices, battlefield systems can be made even more complex, significantly increasing operations'

[1] F. Meneghello et al., 'IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices', IEEE Internet of Things Journal 6, no. 5 (2019): 8182–8201, https://doi.org/10.1109/JIOT.2019.2935189.

[2] 'IoT ~ The Internet of Transformation 2020 | Whitepapers', accessed 20 February 2021, Available from: https://www.juniperresearch.com/white-papers/iot-the-internet-of-transformation-2020.

[3] J. Chudzikiewicz et al., 'The Procedure of Key Distribution in Military IoT Networks', Communications in Computer and Information Science 1039 (2019): 34–47, https://doi.org/10.1007/978-3-030-21952-9_3.

efficiency. Accordingly, it can be stated that they will be defining elements of future areas of operations that can appear in a wide variety of military subsystems such as reconnaissance, logistics, and air defence.[4] These devices must be able to operate in operational environments that are significantly different from civilian circumstances. Examples include limited energy availability, hostile physical and electronic activities (interference), and restrictions on communication channels. Besides, they are also affected by various threats and attacks from cyberspace. Experts believe that many large-scale, multi-vector cyberattacks on IoT devices and systems are expected shortly large-scale, multi-vector cyberattacks, which could cause serious damage and destroy entire operating environments. Accordingly, professionals must pay serious attention to various protection procedures and fault tolerance techniques, even when building systems and networks, because, in an operational environment, this saves not only assets but also lives.

The Open Web Application Security Project (OWASP) compiled an OWASP Top 10 Internet of Things list in 2018 that included the vulnerabilities and weaknesses that could affect IoT devices and systems. These are the following:

- weak, guessable, or hardcoded passwords;
- insecure network services;
- insecure ecosystem interfaces;
- lack of secure update mechanisms;
- use of insecure or outdated components;
- insufficient privacy protection;
- insecure data transfer and storage;
- lack of device management;
- insecure default settings;
- lack of physical hardening.[5]

In this work, the author examines whether these OWASP vulnerabilities exist in IoT devices and systems used in military environments or whether new threats emerge in operational circumstances. To examine and discuss the relationship between the above vulnerabilities and military IoTs, in this work, the author sought answers to the following research questions:

- Do these OWASP vulnerabilities also exist for military IoT devices and systems, or new types of threats emerge in operational environments?
- What are the most common information protection solutions in military environments?

This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and the ÚNKP-20-5-NKE-5 New National Excellence Program of the Ministry of Innovation and Technology.

[4] D. Michalski and P. Bernât, 'Internet of Things in Air and Missile Defence: A System Solution Concept', 2019, https://doi.org/10.1109/MILTECHS.2019.8870070.

[5] 'OWASP Internet of Things Project - OWASP', accessed 20 February 2021, Available from: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10.

Methodology

The author chose the literature review and keyword analysis to answer the research questions, centring on the relevant scientific literature and professional reports. Accordingly, the article focused on the following objectives:

- identification of keywords for IoT devices used in the military environment;
- comprehensive analysis of keywords and topic;
- quantitative analysis based on keyword matches for different threats and vulnerabilities.

The keyword analysis was used to extract relevant information from the analysed literature. Based on the method chosen and the procedure used, the article is divided into the following sections:

- defining the relevant literature
- performing keyword analysis
- examination of the obtained results, drawing conclusions.

The military environment refers to military networks, info-communication and weapons systems, and military operations in this research.

Data

The data used for the research were collected from the Elsevier Scopus database. To obtain relevant information about the topic, the author used the following research queries in the search engine:

- military AND IoT – 550 document results;
- military AND IoT AND threats OR vulnerabilities – 65 document results;
- IoT AND vulnerabilities AND LIMIT-TO (PUBYEAR, 2020) OR LIMIT-TO (PUBYEAR, 2019) OR LIMIT-TO (PUBYEAR, 2018) – 1,557 document results.

The applied keyword analysis results were approved during the analysis of relevant professional reports on the topic.

Tools and analysis

In the research, the author used VOSviewer software to construct and visualize literature and keyword networks to create a map based on bibliographic data from Elsevier Scopus database files. For this, a co-occurrence analysis was applied, which determines the relatedness of the items based on the number of coexisting in the document. From the keyword co-occurrence options (all keywords, author keywords, index keywords), an analysis of all keywords was selected.

1. Research

At the beginning of the research, the author examined the most specific keywords for military IoT. The search query retrieved 550 documents; among them, 270 were found in conference proceedings, 197 in journals, 67 in book series, 8 in books, and 8 in trade journals, which were not relevant to the research. From them, the author identified the most common keywords and examined their relationship to each other. A total of 4213 keywords were identified that could

be found in any of the relevant literature. The 25 most common of these can be found in Table 1, indicating their number of occurrences.

	Keywords	Number of occurrences
1.	Internet of Things	3618
2.	Military applications	1763
3.	Network security	1318
4.	Wireless sensor networks	799
5.	Military communications	580
6.	Sensor nodes	540
7.	Security	473
8.	Energy efficiency	408
9.	Cryptography	376
10.	Unmanned aerial vehicles (uav)	364
11.	Energy utilization	358
12.	Military vehicles	355
13.	Authentication	321
14.	Embedded systems	315
15.	Network architecture	308
16.	Wireless sensor network (wsn)	306
17.	Drones	298
18.	Machine learning	289
19.	Artificial intelligence	277
20.	Automation	270
21.	Blockchain	264
22.	Disaster prevention	260
23.	Internet Protocols	254
24.	Deep learning	251
25.	Quality of Service	247

Table 1: The most common keywords in military IoT[6]

1.1. The connection among the keywords

Of the 4213 keywords that resulted, only the top 100 keywords were included in the relationship analysis, including only those that appeared at least five times in the documents examined. The resulting linkage matrix is shown in Figure 1, where the size of each node showing how frequently a given keyword occurs, while the links represent the co-occurrence relationship between the keywords.

[6] Source: based on the author's research

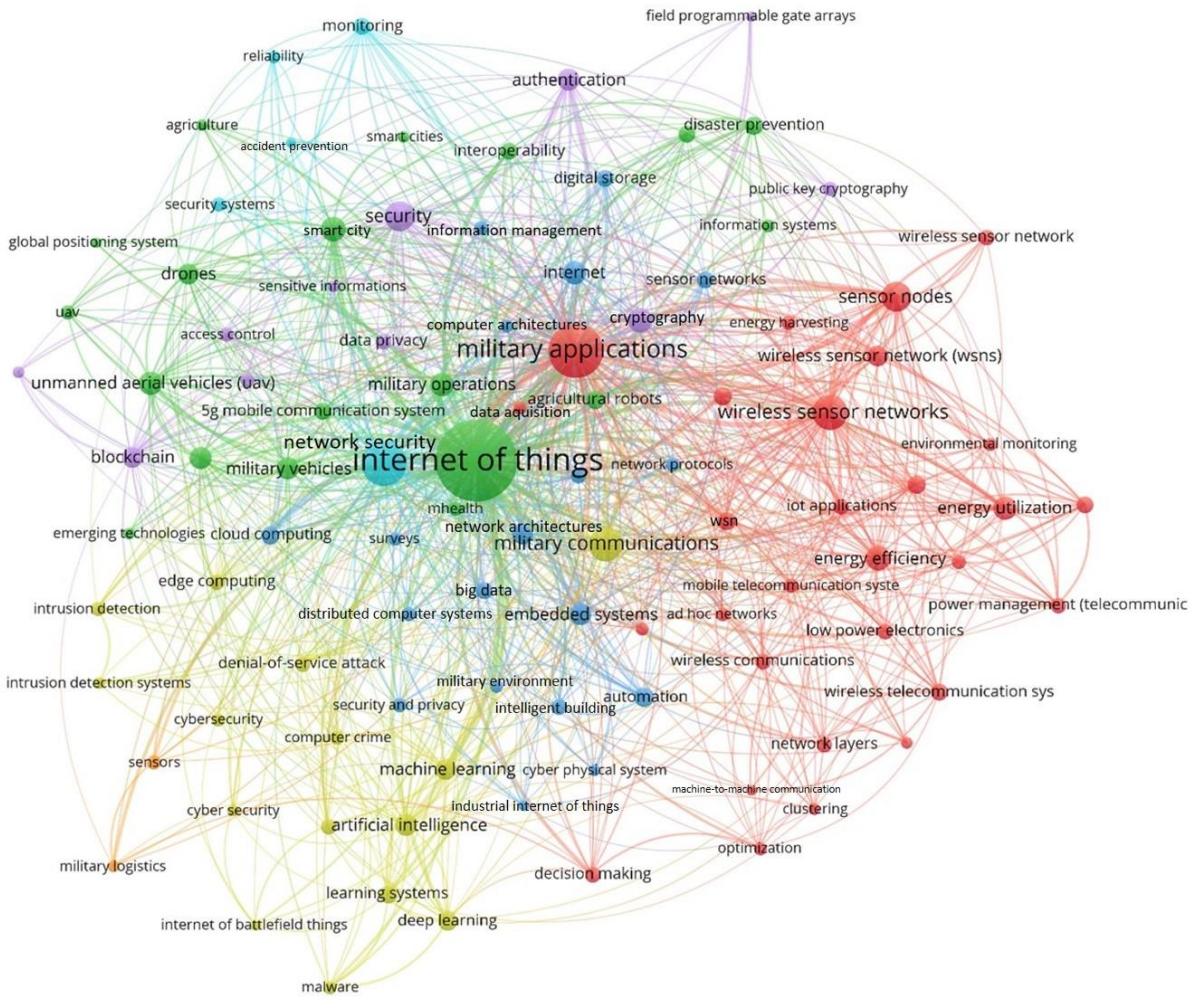

Figure 1: Top 100 keyword network[7]

The top 100 keywords determined by co-occurrence were grouped into seven different clusters that were given different colours based on their association dependencies.

In cluster 1 (green nodes), the central element is the internet of things, and which depicts its relationship to the following military keywords: military operations, military vehicles, unmanned aerial vehicles (UAVs), and drones.

In cluster 2 (red nodes), the central element is military applications, which are significantly connected to wireless sensor networks and communications, machine-to-machine communication, IoT applications, and decision-making.

In cluster 3 (blue nodes), the central element is the embedded system. Its primary military relationship is the military environment, but it is mostly related to the industrial internet of things, automation, big data, information management, network architectures, security and privacy.

In cluster 4 (yellow nodes), the central element is military communication, which is related to the keyword Internet of Battlefield Things but is mostly mentioned together with the terms

[7] Source: based on the author's research made by VOSviewer

artificial intelligence, machine learning, while in terms of threats and protection, cybersecurity, intrusion detection system, computer crime and denial-of-service attack are related to it.

In cluster 5 (purple nodes), the key term is the security which is undividedly connected to cryptography, data privacy, access control, and authentication.

In cluster 6 (light blue nodes), network security is emphasized, and its main connections are security systems, reliability, accident prevention, and monitoring.

In cluster 7 (brown nodes), the significant element is military logistics.

1.2. Joint analysis of the clusters

In the joint analysis of the different clusters, focusing on the military internet of things, the following connections come to the fore.

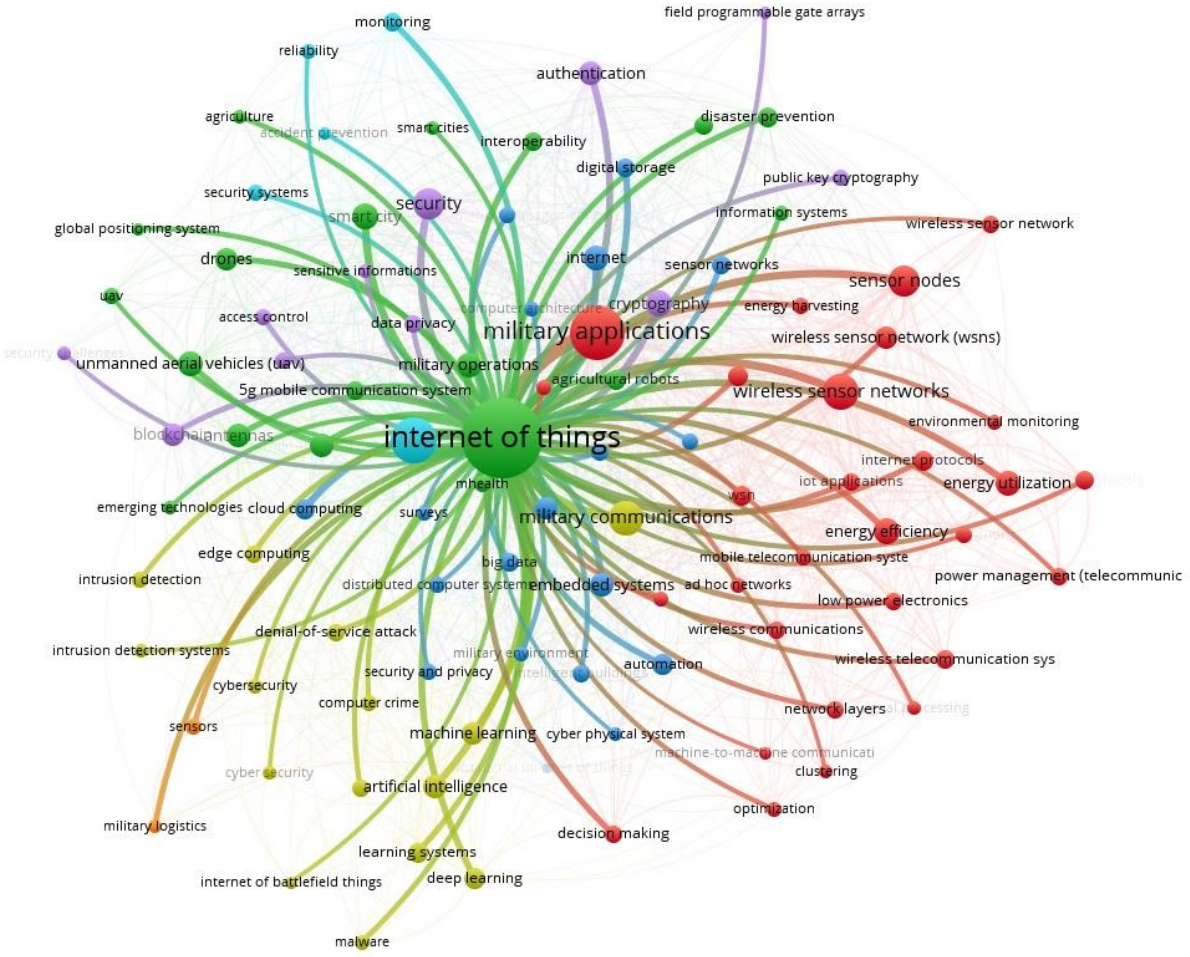

Figure 2: The main connection of military Internet of Things[8]

In this case, the primary military connections are military application, military communication, military operation, but the Internet of Battlefield Things, military logistics, drones, and unmanned aerial vehicles (UAVs) can also be seen there. In terms of communication solutions, the focus is on wireless solutions and wireless sensor network, wireless communication,

[8] Source: based on the author's research made by VOSviewer

wireless telecommunication systems as well. On the security side, there are several keywords in the figure; these are cybersecurity, authentication, cryptography, intrusion detection, monitoring, access control, security systems, security and privacy.

1.3. Identification of potential vulnerabilities

After modifying the research query (military AND IoT AND threats OR vulnerabilities), the author determined how the relevant literature is used to determine potential threats, vulnerabilities, and security solutions according to IoT devices and systems used in military environments. The most common terms related to risks were:

- denial-of-service attack (74);
- security vulnerabilities (52);
- distributed denial of service attack (38);
- computer crime (32);
- security and privacy issues (24);
- cyber vulnerabilities (18);
- software vulnerabilities (18);
- system vulnerability (18);
- user impersonation attacks (18);
- malicious attack (17).

It can be seen from the list that, in some cases, there are links to OWASP IoT Top10 vulnerabilities.

The most common terms of protection that were found in the documents analysed were:

- network security (187);
- security (75);
- authentication (39);
- privacy and security (38);
- cryptography (24);
- data compression (24);
- attack detection (23);
- dos attack detection (23);
- drone security (21);
- intrusion detection system (19).

The privacy protection found in OWASP ToP10 can also be found among the vulnerabilities and the security solutions in the analysed literature, in addition to very different contexts (security and privacy issues, data privacy and securities, privacy by design, security and privacy). Preliminary conclusions could already have been drawn from these results that privacy will be the number one link between IoT devices and systems used in military environments and the OWASP list.

Using the OWASP Top 10 keywords and their equivalents, the search returned the following results:

- “privacy protection” OR “insufficient privacy protection” (44);

- “secure data” OR “insecure data” (24);
- “secure update” OR “insecure update” (22);
- “password” OR “weak password” (21);
- “secure network” OR “insecure network” (18);
- “secure data transfer and storage” OR “insecure data transfer and storage” (15)
- “secure components” OR “insecure components” (13);
- “secure ecosystem” OR “insecure ecosystem” (8);
- “device management” OR “lack of device management” (4);
- “default settings” OR “insecure default settings” (1).

Focusing on the vulnerabilities, the following results were obtained:

- insufficient privacy protection (16);
- weak password (15);
- insecure components (13);
- insecure network (10);
- insecure update (8);
- insecure data transfer and storage (8)
- insecure data (6);
- insecure default settings (1);
- insecure ecosystem (0);
- lack of device management (0).

2. Results

From the above lists, the vulnerabilities identified by OWASP in 2018 do not appear as the most typical threats in the analysed literature. The main reason for this may be that the nature of attacks that threaten information security has changed since then. In some places, the vulnerabilities identified at that time can also be found in the documents, of which the primary connection point is insufficient privacy protection. The principal reason for this may be that much greater emphasis needs to be placed on data protection in military operations, as the success of an operation depends heavily on achieving and maintaining information superiority.

When passwords are used, it is essential that they cannot be decrypted under any circumstances. Each of the literature analysed calls attention to the need to avoid weak, easy-to-guess passwords in any case. Strong passwords are especially important, for example, in wireless body area networks, which are increasingly used by soldiers, where body sensors are placed on soldiers as IoT devices. Password protection of these solutions is particularly important because they provide attack surfaces that attackers can use to obtain information that endangers the wearers' and their companions' lives.[9]

Concerning network security, each of the mentions emphasized the need to avoid the use of insecure networks. In most cases, the principle has been established that reliable and secure IoT

[9] Xin Liu, Ruisheng Zhang, and Mingqi Zhao, ‘A Robust Authentication Scheme with Dynamic Password for Wireless Body Area Networks’, *Computer Networks* 161 (9 October 2019): 220–34, https://doi.org/10.1016/j.comnet.2019.07.003.

(IoBT) networks should be established and operated to disseminate mission-critical information.[10]

In the case of updates, keeping the tools up to date and developing central, efficient update management is a priority in the researched literature. These make it possible to avoid using tools running on insecure software and the use of insecure update mechanisms, thus closing a potential attack surface.

The transport and storage of data is mentioned in the documents examined in accordance with the above elements, and the communication on secure networks will be given a prominent role in them, with which existing data can be protected. The efficiency of storage can be greatly increased by using software protection solutions in all cases in addition to physical protection, thus ensuring the protection of the mass data of the battlefield information.

To perform further analyses, the author performed the third keyword analysis with the IoT AND vulnerabilities AND LIMIT-TO (PUBYEAR, 2020) OR LIMIT-TO (PUBYEAR, 2019) OR LIMIT-TO (PUBYEAR, 2018) research queries, and the results were the following:

- security vulnerabilities (2247);
- distributed denial of service attacks (1940);
- computer crime (1011);
- malware (1005);
- botnet (341);
- software vulnerabilities (220);
- man in the middle attacks (148);
- security problems (146);
- security risks (145);
- security and privacy issues (144).

From the above results based on the researched literature, the most likely threats are not connecting to the OWASP list. The denial-of-service attacks are the first attack vectors that threaten IoT devices and systems used in a military environment. These attacks appear primarily on the Internet of Flying Things (as drones) and in a form that the attacker constantly floods the control centre with messages, making it impossible for the drones and the controller to communicate, thus preventing them from performing their essential function.[11] Compared to the results of the third keyword research and the latest professional reports, the result is that distributed denial of service attacks (DDoS) is one of the most common IoT threats. There are two types of DDoS vulnerabilities. The first is when IoT devices that are not properly protected by manufacturers or are poorly managed by users can be easily attacked by malware and become bots (zombies). Exploiting these security or software vulnerabilities, the attacker remotely controls the devices of the botnet, instructing the IoT elements to perform a DDoS attack. The second is when IoT nodes or control centres will fall victim to DDoS attacks. In this case, the attacker initiates such a large amount of data traffic to the targets, and they become

[10] M. J. Farooq and Q. Zhu, 'On the Secure and Reconfigurable Multi-Layer Network Design for Critical Information Dissemination in the Internet of Battlefield Things (IoBT)', *IEEE Transactions on Wireless Communications* 17, no. 4 (April 2018): 2618–32, https://doi.org/10.1109/TWC.2018.2799860.

[11] A. H. Fitwi et al., 'A Distributed Agent-Based Framework for a Constellation of Drones in a Military Operation', in *2019 Winter Simulation Conference (WSC)*, 2019, 2548–59, https://doi.org/10.1109/WSC40007.2019.9004907.

inaccessible due to congestion. The overwhelmed devices must have a gateway to an insecure network that is not adequately protected.[12] In a military environment, both solutions can cause serious damage, as these types of attacks can kill many people. In the second half of 2020, the number of DDoS weapons (for example SSDP[13] attack; SNMP[14] attack; Portmapper) available on the Internet increased by more than 12%. Due to the increasing prevalence of 5G, the number of smart devices appearing on the Internet has increased significantly, increasing DDoS activities. Another serious problem is that DDoS attacks are not limited to a specific geographic location and can be launched from anywhere in the world.[15] Military IoT devices and networks are also involved in these attacks, which has also appeared several times in the relevant literature, as the DDoS weapons are becoming more sophisticated, making them a potential threat even for severely protected networks.

Considering the above results, the author concluded that one of the biggest problems of IoT systems is privacy protection. Special attention should be paid to fundamental issues such as how data is collected, processed, transported, and stored when building these systems. Privacy concerns appear in all layers of the IoT architecture. These privacy challenges are outlined in the following table:

Layer	Possible attack vectors	Privacy Concerns
Application Layer	• Phishing attacks; • Malicious virus / worm / trojan horse, spyware; • Malicious scripts; • Denial of service; • Software vulnerabilities; • Code injection; • Buffer overflow; • Data aggregation distortion; • Sensitive data permission / manipulation; • Clock skewing; • Data leakage.	• Who has access to the data and information collected by IoT devices and systems? • How can the data stored and managed in the system be used?
Transportation / Network Layer	• DoS attacks; • Spoofing attacks; • Selective forwarding; • Packet replication attacks; • Sinkhole attacks; • Routing information attacks; • Wormhole attacks; • Sybil attacks; • Black hole attacks; • RFID[16] unauthorized access; • Sniffing attacks;	• Is the data transmitted over secure or insecure networks? • Wireless networks, and cloud services are unreliable, can easily become the target of an attack.

[12] A. Srivastava et al., 'Future IoT-Enabled Threats and Vulnerabilities: State of the Art, Challenges, and Future Prospects', *International Journal of Communication Systems* 33, no. 12 (2020), https://doi.org/10.1002/dac.4443.
[13] Simple Service Discovery Protocol
[14] Simple Network Management Protocol
[15]'The State of DDoS Weapons', A10 Networks, accessed 23 March 2021, Available from: https://www.a10networks.com/marketing-comms/reports/state-ddos-weapons/.
[16] Radio Frequency IDentification

	• Traffic analysis attacks.	
Perception / Physical / Sensing Layer	• Node capture / tampering / physical damage attacks; • Physical attacks / tampering; • Hardware trojan; • Denial of Service (DoS) attacks; • Node jamming attacks; • Replication / duplication of a node / device attacks; • Social Engineering; • Malicious code injection attacks; • Malicious node injection; • Camouflage / corrupted / malicious node attack; • False data injection attacks; • Replay attacks (or freshness attacks); • Cryptanalysis attacks and side-channel attacks; • Eavesdropping and interference; • Radio frequency interference on RFIDs; • Sleep deprivation / sleep denial attacks; • Tag cloning or spoofing attacks against RFID tags; • Tracking attacks against RFID tags.	• Many devices collect and even store personal data, such as name, date of birth, customs, and those that are significantly more sensitive to the military topic, such as location, movement routes, health status.

Table 2: Attack vectors and privacy concerns in IoT[17]

The IoT application layer is responsible for providing basic services such as real-time location, collection and analysis of environmental data, network, and layer management. As the documents examined showing, the attack vectors summarized in the table above significantly impact privacy protection so that illegal users reach services with unauthorized access, causing security threats. Attackers can intercept or hijack unattended devices and then obtain sensitive information from clients or application servers with user impersonation attacks, which also appeared in military analyses. The same problem can be exploited by vulnerabilities arising from the development of IoT networks, which allow an attacker to eavesdrop, enter, and manipulate application-layer data. These can cause serious problem for the security of the information stored and processed in the application layer.[18]

The primary reason for the security and cyber vulnerabilities in the network layer may be that proper encryption is not used during operations, which would be essential when using IoT devices. Using encryption can make sensitive information protected; and it ensures that the data is defended even within heterogeneous networks and cannot be accessed by unauthorized persons. The protection prevents that the core network can work undisturbed, even after an attack on a subnet. To avoid these threats, encryption is a basic requirement in military

[17] M.A. Obaidat et al., 'A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures', *Computers* 9, no. 2 (2020), https://doi.org/10.3390/computers9020044.

[18] Y. Li, Y. Li, and J. Liu, 'Discussion on Privacy Issues and Information Security in the Internet of Things', 2020, 4968–72, https://doi.org/10.1109/CCDC49329.2020.9164589.

operations, thus preventing the enemy from eavesdropping or modifying the data.[19] As a result, the research conclusions ranked cryptography among the most important protection solutions.

Recent professional reports intimate that today's IoT vulnerabilities show a similar picture to the results drawn from scientific works. In August 2020, the U.S. Government Accountability Office made a report where the following type of IoT attacks was identified as primary threats:

- Denial of Service attacks;
- Malware attacks;
- Passive Wiretapping;
- Structured query language injection attacks;
- Wardriving attacks;
- Zero-day exploits.[20]

Conclusion

In summary, the list of vulnerabilities identified in OWASP in 2018 for IoT devices used in military environments today is only partially consistent. One of the main reasons for this is that a significant part of the communication during the military tasks' executions are already carried out on secure infocommunication networks. The results obtained in this way are in line with recent professional reports, for which the most common vulnerabilities and threats are the same as the conclusions drawn from scientific works. Nevertheless, due to the increasing use of IoT devices and increasingly sophisticated attack vectors, military IoT networks can also be attacked. According to the analysed literature, DDoS attacks and their consequences (malicious attacks, botnets, unavailable services) are the most likely threats. Privacy protection, which is subject to several threats, has also received serious attention. The primary protection solution to prevent the interception, theft and modification of data is encryption. Encryption is a basic requirement during any such operation, and this precludes insecure network points. Cryptography can help prevent security and privacy issue and user impersonation attacks. Significantly more emphasis needs to be placed on such solutions in the military environment because we can save not only assets but also lives with these solutions.

List of abbreviations

C4ISR	Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance
DDoS	Distributed Denial of Service
DoS	Denial of Service
IoBT	Internet of Battlefield Things
IoFT	Internet of Flying Things
IoT	Internet of Things
MIoT	Military Internet of Things
OWASP	Open Web Application Security Project
RFID	Radio Frequency IDentification
SNMP	Simple Network Management Protocol

[19] F. T. Johnsen et al., 'Application of IoT in Military Operations in a Smart City', in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, 2018, 1–8, https://doi.org/10.1109/ICMCIS.2018.8398690.

[20] United States Government Accountability Office. 'INTERNET OF THINGS: Information on Use by Federal Agencies', August 2020. GAO-20-577

SSDP	Simple Service Discovery Protocol
UAV	Unmanned Aerial Vehicles
WSN	Wireless Sensor Network

CV

Andras TOTH, PhD was born in 1981. He began his military career in an infantry brigade, served several times in foreign missions, twice in Afghanistan, once in Iraq. He has been working at the University of Public Service in Budapest since 2012. Before that, he was a teaching assistant at the National Defence University. He obtained his PhD in network-centric warfare in 2015 and is currently a scholarship holder of the Hungarian Academy of Sciences. He is member and officeholder of the following scientific organisations:

- Hungarian Academy of Sciences (public member)
- Hungarian Association of Military Science (member of the electoral board)
- Scientific Association for Infocommunications, Cyber Security Committee (vice-president)
- Tivadar Puskás Technical College for Advanced Studies (president)
- University Scientific Students' Council (president)

Email address: toth.hir.andras@uni-nke.hu