

The IoT further complicates the cyberdefense mission of cyberarmies

BOUKERS Saâd ¹, BELKHIR Abdelkader ²

¹ USTHB, Faculty of Electronics and Computer Science, Computer Science department (Algeria), Saad.BOUKERS@Gmail.com

² USTHB, Faculty of Electronics and Computer Science, Computer Science department (Algeria), BELKHIR@lsi-usthb.dz

Received: 30/01/2022

Accepted: 10/05/2022

Published: 06./06/2022

Abstract:

Starting from the idea that every object connected to the Internet can be a source of threat to data security, material resources and reputation. In fact, the expansion of the Internet network to Things is a natural evolution of innovation in Information and Communication Technologies field (ICT). Nowadays, every connected object can be identified as a single, autonomous entity which is very sensitive to its environment.

In recent years, connected objects have multiplied in our daily lives and have considerably expended the attack surface in cyberspace. In addition, we notice a strong network interaction and permanent connectivity with a very high volume of data, which have further complicated the cyberdefense mission of the cyberarmies.

Keywords: Internet of Things; Cyberspace; Cybersecurity; Cybercriminality; Cybercombatant.

Corresponding authors: BOUKERS Saâd and BELKHIR Abdelkader

1. INTRODUCTION

The Internet of Things (IoT) continues to evolve in technologies, applications and usage from year to year. However, this evolution has further complicated the understanding of the limits between microcomputers and these connected objects and between the Internet and IoT for States, companies and individuals.

This rapid evolution has given rise to a **new complexity** as a result of its modification of the environment of human beings and organizations as well as their procedures and work strategies in general and those of military institutions in a particular way.

This article is dedicated mainly to the presentation of this new complexity and how can we manage it on a daily basis, especially when it is omnipresent and invisible.

The second part of this article presents the concepts of cyberspace, cybersecurity, cybercrime and cyberdefense. The third part deals with the Internet of Things (IoT) concept, its application fields and its challenges to security. The fourth and fifth parts will be devoted respectively to certain recommendations and a conclusion.

2. CONCEPTS

The objective of this part is to present some concepts allowing us to have a general idea about the IoT environment. The four relevant concepts deemed important are cyberspace, cybercriminality, cyberdefense and cybersecurity.

2.1 Cyberspace

Cyberspace is a virtual space, created by the global interconnection of all microcomputers and connected objects. Cyberspace has become the fifth space of war, after land, sea, air and space (BOUKERS, Le DICDTIC3, 2021). Cyberspace is totally connected, omnipresent, easy to access, complex and variable according to its actors. It is also a space for exchanges and confrontations between actors, especially as it includes multiple very versatile opponents.

Exchanges and developments are very rapid in a cyberspace which is highly

decentralized. Cyberspace, therefore, is an advantageous, risky and dangerous space that can contain complex cyberattacks that can paralyze an entire country or a group of countries.

2.2 Cybercriminality

The European Commission defines "cybercriminality" by three categories of criminal activity:

- Traditional forms of crime (fraud and informatics falsification = scams, fake payment cards, etc.)
- The dissemination of illegal content by electronic means (sexual violence against children, incitement to racial hatred, etc.).
- Offenses specific to electronic networks, i.e, attacks targeting information systems, denial of service and hacking.

« We can distinguish five categories of infractions in cyberspace: infractions against press law, child pornography, piracy, fraud and counterfeiting » (Frédérique, 2009).

In the legal framework, it is noted that the European Commission has tried to include all possible criminal acts in its definition of cybercriminality so as not to leave loopholes through which criminals can escape sanctions. However, with the rapid evolution of ICTs and their services, criminal activities have increasingly developed. Therefore, it is recommended to the regulatory institutions to be very vigilant by ensuring all the necessary updates and to regularly enforce them because the common feature of many offenses is permanent escalation.

According to researcher Colin ROSE, « *Cybercriminality is the third major threat to major powers, after chemical, bacteriological and nuclear weapons* » (BOOS, 2016).

2.3 Cyberdefense

Cyber defense is the set of material and immaterial means put in place by a State to protect and to defend the essential of information systems of its military and civilian institutions against the risks and dangers of cyberspace. It is a crucial issue for all cyberarmies, of their countries in general and the sovereignty of their digital spaces in particular.

2.4 Cybersecurity

Cybersecurity is the strategy and actions associated with the security risk management processes followed by organizations and States with the aim of protecting the confidentiality, integrity and availability of sensitive data and assets used in cyberspace. This concept includes guidelines, rules, policies and a set of technological controls, tools and training to best protect the cyber environment and its users (SCHATZ, BASHROUSH, & WALL, 2017).

For Doctor Camille de Sagazan, this definition seems broad enough to reconcile, as far as necessary, the different historical of informatics security (CAMILLE, 2020).

For BOUKERS Saâd, « *cybersecurity is a set of technologies, processes and good practices aiming to protecting hardware, data and software against cyberattacks, that is, attacks from cyberspace* » (BOUKERS, Introduction To Micro-Informatics, 2021).

The three components of cybersecurity are cyberdefense, Information System (IS) security and the fight against cybercrime.

Cybersecurity is also an important issue for citizens and companies, who must be able to exploit all the opportunities offered by cyberspace without major risk. It is also a crucial issue for States, which must be able to maintain their sovereignty.

The difference between cybersecurity and security is that security also deals with the security of material resources against environmental, organizational and human threats.

It should be noted that the security or cybersecurity of an information system is measured by the security of its weakest element. It is for this reason that an effective security policy must necessarily take into consideration the five areas of computer security mentioned in the following figure:

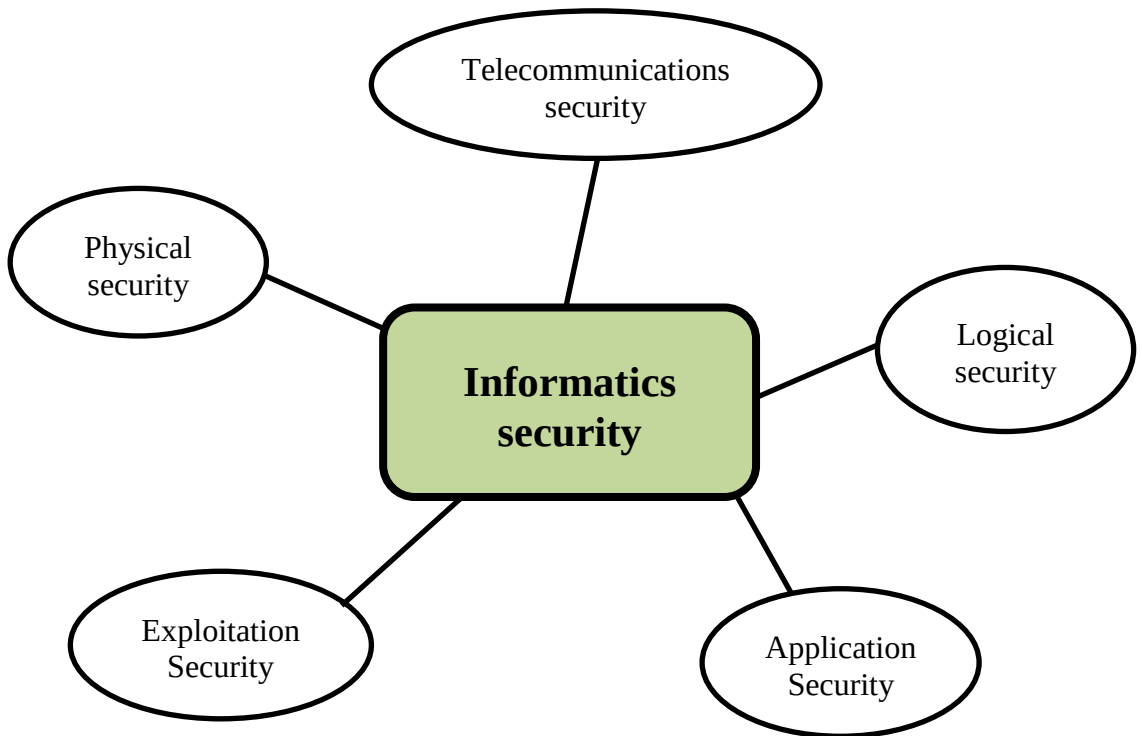


Figure 01 : The main domains of informatics security

Source : Par les auteurs

In addition, global informatics security must be accompanied by evolving regulations in order to effectively fight cybercrime. It must also be accompanied by good information management at its heart is the management of information-related risks, etc.

It should be noted that the information security management system is the main subject of the ISO 27001 standard, which defines its characteristics (Feel agile).

Figure 02 : IoT related image

Source : (Pixabay, Pixabay)

These are sometimes personal equipments (geolocatable glasses, watches, bracelets, thermometers, etc.), but also equipment for family, industrial and military use like refrigerators, vehicles, drones, video protection cameras, locks, alarms, smoke detectors, etc.

The Internet of Things therefore represents all connected objects capable of exchanging data with other physical or digital entities.

The European Institute IDATEDigiWorld, specializing in the telecoms, Internet, media and digital territories markets, announced the total of 11.2 billion connected objects worldwide in 2017. It also forecasts a growth rate of 10% per year, to reach a fleet of 35 billion units worldwide in 2030. (IDATE, 1918)

It should be noted that the number of connected objects is in rapid and continuous evolution. It requires a huge addressing capacity especially in the next decades. Fortunately, IPv6 is there. Thanks to addresses of 128 bits instead of 32 bits, IPv6 has a much larger address space than IPv4 (nearly 100 billion billion times more). It allows a space of 2^{128} IP addresses.

3.2 Application areas of IoT

The IoT has multiple applications and objects covering various fields, citing as examples:

Agriculture: use of captors for real-time monitoring of harvests progress and cattle monitoring using geolocation chips, etc.

Home automation: creation of smart cities via the creation of smart buildings capable of adapting to variations in environmental parameters such as light and temperature. The IoT will also allow watering, closing windows and lighting based on information transmitted by the captors. It makes it possible to better manage traffic flows, optimize lighting, control energy consumption, etc.

Security: The IoT offers the use of intrusion detectors, the use of surveillance videos as tools to help investigators and even the tracking of

criminals for possible control or arrest in real time, etc.

Health: The IoT helps improve innovation and reduce expenses in the health sector. It will offer increased safety to patients at risk by giving them the possibility of being monitored remotely, which will also result in a reduction in hospital costs.

Industry: In the field of industry, the IoT makes it possible to carry out measurements, prognoses and predictions of breakdowns as well as remote troubleshooting. It also makes it possible to remotely monitor and control the operation of the machines by giving them, for example, the possibility of triggering a replenishment of raw materials themselves. As we can cite the example of the use of drones by the film industry. Similarly, the industrial sector also uses IoT to reduce risk and work stoppages. It also uses “smart workspaces” to improve productivity and efficiency.

Mobility: The IoT allows the optimization of means of transport, the geolocation of vehicles, the dissemination of information on public transport and the availability of places in car parks, etc.

Military: Drones as connected objects represent a new page in the history of aerospace. They are able to fly and carry out missions without human presence on board. The three main categories of military missions entrusted to drones in the military domain are surveillance and intelligence, combat support and combat.



Figure 03 : Image related to a type of ghost drone.

Source : (Pixabay, Pixabay)

Examples of the use of military drones: Dropping survival packs (parachuted) to advanced commandos, monitoring enemy movements on the road, laser designation of a target on the ground allowing firing from a weapon plane and communications relay between a ground station and a high altitude aircraft.

Drones are also used in other domains including the following missions:

- Maritime and urban surveillance;
- Monitoring of demonstrations, road traffic and the transport of dangerous materials;
- Research and monitoring of forest fires, floods, storms, earthquakes, avalanches, volcanoes and tornadoes;
- Search and rescue in sea, mountains, desert etc.;
- Inspection infrastructures such as bridges, viaducts and dams;
- Detection of toxic gases and radiation;
- Study of the atmosphere, soils (geology) and oceans;
- Meteorological studies and forecasts...etc.

3.3 - The challenges of the Internet of Things

From now on the IoT will considerably challenge States and Companies alike, as it has imposedely occupied an important position in their IoT market, becoming a factor of productivity and creativity, affecting practically all areas of human activity.

In general, the challenge of the IoT can be assessed under three aspects, comfort aspect, economic aspect and security aspect:

Comfort aspect: It contributes to improving comfort by simplifying the daily professional and private life of people.

Economic aspect: It appears in two complementary forms:

- The existence of a product market in the form of physical objects and software like systems and applications estimated at 500 to 600 billion USD worldwide between 2020 and 2025 (François, Gerin; Jean-Pierre, Hauet;

Suzanne, Debaille; Alain, Brenac; Xu, Yihong, 2017, p. 6).

- The creation of value in the form of modernization of the economy, improvement of productivity, reduction of supply costs, etc. Here, value creation is estimated at 2,000 to 2,500 billion USD in 2025 (François, Gerin; Jean-Pierre, Hauet; Suzanne, Debaille; Alain, Brenac; Xu, Yihong, 2017, p. 7).

Security aspect: It participates as a tool to help investigators, monitor the health of people, help and orientation in sport as well as the monitoring and tracking of criminals in real time, etc.

Today, no sector of economic activity escapes the challenge of connected objects. The challenge is often expressed directly in terms of:

- Productivity in industry with the Industrial Internet of Things and in agriculture.
- Quality of the services provided, in the fields of weather, environment, transport and infrastructure.
- Safety and comfort in the fields of health and home automation.
- New services and new hobbies (sports, communicating worn objects, etc.).
- Maintaining employment for object manufacturers and application development companies and even recruiting new employees.
- Development of communication means.
- New data processing methods.
- More efficient innovation and reduced time to market, etc.

3.4 Information Security and the Internet of Things

With the IoT, the playground for criminals is expanding every day. Connected objects have their advantages in terms of economy, comfort and security. However, they can also be sources of threats to States, businesses and private lives of individuals and the strengthening of information security is the only solution.

It should be remembered that the four main objectives of informatics security are integrity, confidentiality, availability and non-repudiation.

- **Integrity** consists of ensuring an exact and unaltered representation of information or a system. It ensures that an information or a system can only

be modified by authorized users or processes.

- **Confidentiality** consists in making the information communicated from an exchange of information unintelligible to a person who is not concerned by this exchange. The confidentiality of the data transmitted or also stored is ensured by the use of cryptographic techniques.
- **Availability** is the characteristic of an informatics system that is able to always maintain its service without interruption.
- **Non-repudiation** (or non-disavowal) is the characteristic of an informatics system which is able to guarantee that a transaction carried out cannot be denied by one of its participants.

It should be noted that **authentication** is a procedure which consists in ensuring that only authorized entities (human being or another system, etc.) have access to the requested resource (systems, networks, applications, services, etc.). It is therefore a mechanism that ensures confidentiality by controlling access.

Starting from the fact that zero risk does not exist in informatics, an informatics system is never secure forever. New informatics attack techniques appear regularly, new connected objects and new flaws in software and equipment are discovered frequently.

In information security, risk is perceived as a threat that exploits vulnerability with negative impacts.

$$\text{Risk} = \frac{\text{Threat} \times \text{Vulnerability}}{\text{Countermeasure}}$$

This means that the risks of a third party can become the risks of all linked or involved third parties.

- A **threat** is a possible event (of non-zero probability) and feared likely to compromise the security of an informatics system. Threats can combine with each other to form an attack scenario according to a sequence.

- A **vulnerability** is a flaw, weakness or breach in software or in its configuration or installation allowing a cybercriminal to undermine one of the main objectives of informatics security (integrity, confidentiality, availability and non-repudiation).

A vulnerability can also be:

- Environmental (humidity, temperature, fires, floods, earthquakes, etc.);
- Organizational (lack of backup plan, lack of password management policy, etc.);
- Physical (lack of physical access control procedure to premises, etc.);
- Human (lack of user awareness and training in safety, etc.).

Other basic examples of vulnerabilities

- Installation of software without a user license.
- The continuity of using software whose license period has expired.
- Operating system not updated.
- Application made by a developer, without considering the security aspects of the application, from its design to its implementation.

- The **countermeasure** is a device encompassing all the actions implemented to prevent threats.

Examples of countermeasures

- The first countermeasure is prevention through awareness campaigns for all employees using the company's network of the risks, threats and dangers of cyberspace.
- Establish a policy for physical access and updating of operating systems and the application base.
- Drafting of a charter for the use of informatics resources and digital tools.
- Antivirus installation.
- Purchase of software with user licenses in order to ensure their automatic

updating (one software = one license).

- Use of proven security solutions (firewall, antivirus).
- Have sufficient staff and high technical skills in informatics security field.
- Encryption of data and information exchanges using encryption software.
- Analysis by an antivirus of all USB media before their use.
- Disable automatic execution of removable media from computers.
- Shut down computers during periods of prolonged inactivity (night, weekend, holidays, etc.).
- Surveillance and monitoring of the operating system, in particular by using event logs, to react to suspicious events (connection of a user outside his usual hours, massive transfer of data outside the company, attempts connection to an inactive account, etc.).
- The company must empower its collaborators by informing them of the consequences incurred by the company in case its information system vulnerability. This means that company's IT security is the concern of all its collaborators.
- Apply best practices.
- Regular complete audit of the company's informatics security, etc.

Informatics security researchers have shown that it is possible to remotely compromise connected watches in order to take control of their captors (microphone, heart rate measurement, etc.) or access the data exchanged between the watch and the Smartphone to which it is connected.

These vulnerabilities could be usefully exploited for malicious purposes in the direction of a previously targeted employee of a sensitive company, and give access to some of their strategic information (DGSI, 2019, p. 3).

So, in terms of information security, the IoT forces us to ask certain questions: Who will have access to the object and how will it be established and tested? What are its threats? How are they to be mitigated? Who should be notified in case of an attack or the discovery of vulnerability? What is the update process in the event of vulnerability? What personal information is collected, stored and/or processed? With Whom the data will be shared? Do people whose information is collected know what is collected and used? Do they give their consent? Etc.

It should be warned that that in 2021, researchers from the Avira Protection Laboratory observed a 50% increase in attacks targeting connected objects compared to 2020 (Vukcevic, 2021).

4. Recommendations

4.1 Cybercombatant Training Recommendations

- The first recommendation: Knowing that the first element necessary to ensure good security is not technological, but human. The first recommendation is **prevention** through training and awareness campaigns on the risks, threats and dangers of cyberspace for all employees of military institutions who use informatics tool in their work.
- The second recommendation: Training and certification of cybercombatants in application development, since the security of an application is practiced at all stages of its life, from design to implementation. Most of the security materializes in the code, from the framework provided by the design. At the end, security materializes through the monitoring of daily operations, when the application is put into production. It is also imperative that the cybercombatant in application development master all the security concepts in development.
- Third recommendation: Training and certification of cybercombatants in database administration and security.
- The fourth recommendation: Training and certification of cybercombatants in network administration and security.

4.2 IoT Recommendations

In addition to the standard countermeasures mentioned above and in order to reduce the risks associated with the use of connected objects in the workplace, it is recommended to follow and apply the following best practices (DGSI, 2019, pp. 4-5).:

For industrial connected objects

- List and install a watch on the vulnerabilities of connected objects in activity in the company.
- Question the suppliers of connected objects on the security measures

implemented in their products. If possible, compare different models of connected objects by integrating a technical evaluation of security level.

- Engage in a risk analysis before authorizing and deploying connected objects on the company's information systems.
- Create Wi-Fi or wired networks dedicated to the use of connected and partitioned objects.

For consumer connected objects

- Supervise the use of personal connected objects in a charter of good practices or integrate it into the information systems security policy (ISSP).
- Make employees aware of the vulnerabilities linked to connected objects and in particular the personal data that they are required to collect, generate and transfer to Cloud services.

In a general way:

- Disable the administration interface on the Internet, if proposed by the product supplier as far as possible change the default passwords if necessary.
- Regularly deploy product updates, when these are proposed by the supplier.

4. CONCLUSION

In conclusion, the Internet of Things is a natural evolution of ICTs and their services. It is a fast-evolving, innovative and growth-enhancing field for ICT applications and equipment. In fact IoT brings comfort to human beings on a professional and personal level. It is also complex with a strong network dimension and a strong system dimension.

The Internet of Things therefore opens up an ultra-connected environment, the fact that led to expanding the attack surface in cyberspace through its openness, geographical deployment, scalability, permanent connectivity and large volume of data. Imagine the impact of the enemy taking control of a drone remotely or on a video surveillance camera at a strategic military site or on any other object used in the military field. So, it is clear, that the IoT further complicates the cyber defense mission of cyberarmies around the world.

5. Bibliography

- BOOS, R. (2016). La lutte contre la cybercriminalité au regard de l'action de l'état. *HALL open science*, 21.
- BOUKERS, S. (2021). *Introduction To Micro-Informatics* (1ère édition ed.). Baraki, Alger, Algérie: Mitidja Impression.
- BOUKERS, S. (2021). *Le DICDTIC3* (éd. 1ère édition). Baraki, Alger, Algérie: Mitidja Impression.
- CAMILLE, d. S. (2020). *Introduction à la cybersécurité*. Paris, France: Ellipses Edition Marketing S.A.
- DGSI. (2019). *INGERENCE ECONOMIQUE*. Consulted on January 29, 2029, on [prefectures-regions.gouv.fr](https://www.prefectures-regions.gouv.fr): <https://www.prefectures-regions.gouv.fr/ile-de-france/content/download/54854/362257/file/Flash-n49-janvier-2019.pdf>
- Feel agile. (s.d.). *Feel agile*. Consulted on October 04, 2021, on feelagile.com: <https://feelagile.com/quest-ce-quun-smsi/>
- François, Gerin; Jean-Pierre, Hauet; Suzanne, Debaille; Alain, Brenac; Xu, Yihong. (2017). *Internet des objets 2018 - Rapport Principal*. Consulted on January 29, 2029, on bscw.5g-ppp.eu: <https://bscw.5g-ppp.eu/pub/bscw.cgi/d208247/IoT%20Rapport%20Abstract.pdf>
- Frédérique, C. (2009). Les politiques publiques de lutte contre la cybersriminalité. *AJ Pénal*, 101.
- Hewlett Packard, e. (s.d.). *L'Internet des Objets: état des lieux et perspectives*. Consulted on January 29, 2029, on [dsih.fr](https://www.dsih.fr): https://www.dsih.fr/images/Rapport-etude_IoT_ARUBA-1.pdf
- IDATE. (1918, Janvier 31). *IoT : Un marché qui tient sa promesse d'une croissance de 10% par an grâce au dynamisme des*

marchés industriels. Consulted on January 29, 2029, on idate.org: <https://fr.idate.org/marche-iot-2018/>

PIPAME, F. (2018). *Marchés des objets connectés à destination du grand public*. (M. d. l'économie, Éd.) Consulted on January 29, 2029, on Entreprises.gouv.fr - Le portail de la Direction Générale des Entreprises: <https://www.entreprises.gouv.fr/files/files/01-nouveau-portail/etudes-statistiques/etudes/2018-05-24-etude-objets-connectes.pdf>

Pixabay. (s.d.). *Pixabay*. Consulted on October 14, 2021, on pixabay.com: <https://pixabay.com/fr/photos/drone-fant%c3%b4me-dji-professionnel-1112752/>

Pixabay. (s.d.). *Pixabay*. Consulted on Octpber 13, 2021, on pixabay.com: <https://pixabay.com/fr/vectors/r%c3%a9seau-iot-internet-des-objets-782707/>

SCHATZ, D., BASHROUSH, R., & WALL, J. (2017). Towards a More Representatives Definition of Cyber Security. *The journal of Digital Forensics, Security and Law*, 12(2), 66.

UIT. (2012, 06). *Présentation générale de l'Internet des objets, Recommandation UIT-T Y.2060*. (UIT, Éd.) Consulted on January 29, 2029, on www.itu.int: https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-Y.2060-201206-I!!PDF-F&type=items

Vukcevic, A. (2021, Mars 8). *Prédictions : les menaces de l'IoT en 2021*. Consulted on October 13, 2021, on journaldunet.com: <https://www.journaldunet.com/ebusiness/internet-mobile/1498505-predictions-les-menaces-de-l-iot-en-2021/>