

From Spread Spectrum Communications to Artificial Intelligence – A Continuous Way Where Information and Communication Technology Supports the World Progress in the Fight Against Interference and Cyber Attacks



Prof. Eng. Ph.D. Victor GREU

Abstract

The paper analyses the increasing role of communications and AI in the context of World unprecedented challenges and crises, especially for fighting against interference and cyber attacks (as a result of cumulating/interfering factors, including some of them unknown, unexpected or undefined- **like social media underground influence on person behaviour**). This worrying complex context is the reason why we considered useful (and actual!) to recall some historical evolutions of ICT and communications, including even relative recent ones from our paper [6], just to emphasise the amazing speed of World colliding crises and then the necessity to learn from history and use all the resources for surviving. The analysis is first focused on features and evolution of spread spectrum systems (SSS), from 1932 patents and Claude Shannon theory to Irwin M. Jacobs (QUALCOMM founder) fascinating contributions to CDMA and cellular standards, including also some aspects about our research on SSS impact in Romania (from 1979). Technical details on interference mitigation, spectrum monitoring, software/AI advances and elusive interferences, are approached, based on [8]. The AI role could increase, in our full of uncertainties World, as today we have to be prepared for any kind of „interference”. We also analysed some advances in the complicated area of cyber security, as approached by [10], where deep learning and neural networks have amazing performances. Here the optimization solution is much complicate and difficult to certainly find and interpret which is the attack cause/author and often we want to know which packets lead to the attack, where they come from, or which are malicious. The search of unexpected threats between billions of bits/sources/persons is a kind of nightmare. One of the explainable AI techniques that have been directed to cyber security problems with domain-specific knowledge is TRUSTEE and similar results are given by SHAP. Our main conclusion is that, using all power of AI, the human intelligence (HI) must remain the main reference for such mission critical applications and AI development, advance or use [16][22]. We can see how complicate is the fight with elusive interference or cyber attacks and how “long and winding road” must be done, even with the fast AI advances which are, of course, the expected solutions where the complexity and Big Data are more present, but **it is worth to notice the HI which “supports” both sides of the competition. SSS opened a specific way for AI approach of signals structure and processing [2][5][6], with impact beyond this area. Some ingredients of such approaches could be still seen from the technical features of SSS/CDMA example.** Even from 2013, we observed the relevance of ICT/SSS advances for the emerging World challenges [6]: “CDMA is also a model... The essential observation could be extracted just from the Irwin Jacobs’s initial idea: we can optimize a process by reusing the pauses, i.e., the time”. We could notice, after 10 years of World “progress”, not only the right direction, but also **the painful actuality**, opportunity and even the necessary holistic approach of all useful resources to mitigate the aggressive World challenges: <<We have also to adapt and face the new challenges of life, including the „side effects” of the technological progress, using the CDMA/SSS models, which „compute” and provide any „slice” of **all the resources** for every user and network, in a precise and negotiated order, avoiding interference and conflicts... A subsequent lesson people could learn from CDMA is to better and wiser live with the neighbours and environment, reducing the „mutual interference” and being more tolerant on a rational...basis. The „secure” feature of CDMA/SSS could help us to respect privacy and personal information, such idea being very actual as social networks already reveal their risks on privacy and overdoing>>.

Beyond the transparence of the presented technical features (anti interference, anti cyber attacks etc.) to rational hints about the generic interferences/attacks at the human essential struggle for survival, we should understand, still, the potential of ICT/AI and HI to support our World against the seen and even unexpected threats, which could be optimally used only by spreading the necessary “refined knowledge inside”, before the

threats advance and before... being too late! But we have to not forget to imagine and be prepared, what if Internet, Communications or AI does not work, at least partially, for a while...one day, as some interferences/incidents already showed!

Keywords: spread spectrum systems, interference, cyber attacks, artificial intelligence, deep learning, neural networks, decision trees, network intrusion detection system, frequency hopping, knowledge-based society

JEL Classification: L63; L86; M15; O31; O33

***“The true sign of intelligence is not knowledge but imagination”
- Albert Einstein***

1. Learning from history and from the ways communications are fighting, with advanced technologies, World invisible threats like interference

Our beautiful Earth is always an inherent source of inspiration and wondering, first due to the unlimited humankind potential to create new and sometimes unexpected “events” and products.

How wonderful it would be if such “events” and products could bring only joy and benefits for everyone ... everywhere!

Unfortunately, what we could see almost every day, in our World of challenges and crises, is more and more different and ... worrying!

Even if considering the subjectivism of such impressions, it is still obvious that the actual World crises and challenges generate unprecedented levels of concern for most people and incumbents, just reminding the recent aggressive consequences of global warming (climate changes), but also the progressive Earth resources fading, social unbalances or geopolitical/security crises, threats against democracy or changes in human behaviour/habit values [16][19][15][17][18][23].

This worrying complex context is the reason why we considered useful (and actual!) to recall some historical evolutions of ICT and communications, including even relative recent ones from our paper [6], just to emphasize the amazing speed of World colliding crises and then the necessity to learn from history and use all the resources for surviving.

On the other hand, also recently [14], we observed, one more time, **some indirect ways the ICT could leverage the World progress and mitigate the above challenges, by deeply innovating its advances.**

We also repeatedly stressed that any World progress should consider the information and communication technology (ICT) crucial role, as ICT became the main driving factor of the human society by the complex consequences of its products, applications and services, when supporting the Information Society (IS) on the way towards the Knowledge Based Society (KBS), while the average development is the result of global tendencies/innovations, including knowledge refining everywhere [21][18].

One of the most interesting ways ICT contribute to this World fight/progress is an indirectly one, recalling that its proven efficient/automated models and algorithms of development and proliferation could be largely used/lend to other fields of human activity [22].

As our World complex, complicate and fast changing context we are in could be, sometimes, perceived and studied as a result of cumulating/interfering factors, including some of them unknown, unexpected or undefined (**like social media underground influence on person behaviour**), the paper analysis is intended to reveal some ICT ways/solutions for interference (as general meaning) mitigation, including communications and artificial

intelligence (AI) advanced results, while the possibilities to use these approaches in other areas are relevant.

This way, our opinion is that analysing some models/technologies of the ways ICT and the communications equipments/networks fight interference is not only a useful technical example of ICT innovation/progress, but also an inspiration and even instrument for the complex and difficult approach of other similar World and humankind emerging challenges.

First of all, we should shortly recall some basic or historical moments of communications equipments/networks (and generally of ICT), where solutions to mitigate interference and other vulnerabilities were in focus.

We have to mention that the aim of this paper is not only to show the role of such historical moments, from the point of view of science and technology evolutions, but mainly to reveal the context models (including AI) which could be beneficently extended to other World challenges, emergent or foreseen, where “unexpected interference”, as a generic, but not necessary technical concept, could be a threat, as lately, in our World of crises, we have encountered, especially through social media (like TikTok) or other kinds of cyber-attacks or hybrid war.

As, few years ago, the subject of „interference resistance” was presented in a new approach [3], adding some details to this context could be interesting and useful for the paper mentioned aim about the communications development.

It is well known that communications development, while providing more and more benefits, keeps a so called “Achile’s heal” vulnerability, by the fact that any communication, especially for defence and security purposes, could inherently offer to the enemy or to the third party some information, at least by the simple using or radiation of energy, which is more than obvious in the case of radiocommunications.

We have to notice that, even in the non-military applications, the sensitivity or susceptibility to electromagnetic interference is also an important vulnerability to be technically approached and mitigated, i.e., the analysis and the eventual solutions are important and of general interest, from the point of view of electromagnetic compatibility.

Still, the protection of military radio communications, from their early moments, led to the first ideas to avoid interference or information interception, about the time of World War I, although, much later, a diversity of patents was claimed, one of them getting additional benefit due to a famous actress [3]:

“Actress Hedy Lamarr famously co-patented a widely used secure communication technology, but popular accounts overlook many predecessors... It is true that Lamarr and her unlikely partner, the radical modernist composer George Antheil, hold a patent for an important radio-transmission method that finds its way into several modern communications technologies, including Bluetooth. But it is equally true that their patent was hardly the first in this area. It is further true that the earliest operational systems employing this technique were created after World War II independently of their patent, and the essential idea can be traced back nearly to the birth of radio itself... On August 11, 1942, Lamarr and Antheil received U.S. Patent 2,292,387 (issued to Lamarr under her married name, Hedy Markey) for a “secret communication system.”

Further, without adding too much such episodes, we have noticed a relevant and concluding example:

<<Dutch inventor Willem Broertjes, who on October 11, 1929, submitted a patent application in Germany for a “Method of Maintaining Secrecy in the Transmission of Wireless Telegraph Messages.” A month later Broertjes filed an application in America, and in 1932 he was awarded U.S. Patent 1,869,659. In it, he writes that

The known methods of maintaining secrecy operate, in most cases, with codes or cryptograms and with a periodically modified transmission frequency, which is

received by means of a receiving apparatus, the tuning of which is modified in synchronism.

According to Broertjes, then, the idea of changing transmission frequencies is already commonplace, but he argues that this approach does not prevent the interception and decipherment of the message, because a broadband receiver could pick up all the frequencies. As Lamarr and Antheil did later, Broertjes then proposes a system in which a number of “working frequencies,” known to the sender and receiver alone, can be varied in a “random or variable manner,” or even left out.>>

The reality, about the spread spectrum systems (SSS) in general, is much more complex and fuller of scientific and technical relevant details, we also researched, with some national level results [7][2][27], while we have introduced them in the university teaching process in the Military Technical Academy [5][28][29][30].

The specialists mainly recognize that the scientific basics of communications with SSS, after some steps of patents evolution, were mainly given, in 1945, by Claude Shannon formula/equation of channel capacity and on the other hand the technical definitional requirements of SSS could be essentially expressed by 2 requirements and some performance features [26][24][25][2][27]:

- A. The system bandwidth >> information band (the multiplicity factor >> 1);
- B. A noise-like (pseudo noise -PN) spreading law, independent of information, should be used.

Also, the performance features of SSS include:

- a. Anti-jam resistance;
- b. Low probability of interception (LPI), due to PN use;
- c. Multiple access capacity (code division multiple access - CDMA);
- d. Use of diverse techniques of spreading the spectrum (direct sequence- DS; frequency hopping - FH; time hopping - TH; hybrid techniques).

The key factor of secret and reliable synchronization between receiver and transmitter is the most complex and difficult part, especially for getting antijam, anti-intercept features, which is not the case of non-military applications [26][2][5][27].

We should mention that much of non-military applications, as CDMA and FH (including but not limiting to Bluetooth, WiFi, WiMax or OFDM), expanded in almost all modern communications, including 2G to 5G, do not truly (maximally) respect/provide the above-mentioned definitional requirements of SSS and consequently the performances.

We also analysed the requirements and some performance features of SSS, with some technical details, in [6]:

<<... we may find the theoretical origins of CDMA, inside a more complex concept named „spread spectrum systems” (SSS), which was founded by Claude Shannon in 1945.

In 1945 Shannon wrote a paper, “A Mathematical Theory of Cryptography”, but never published because it was stamped SECRET. A „cleared” version was still published in 1949, as „Communication theory of secrecy systems”. Again simply, we may say that Shannon theoretical model (equation) postulated SSS as a wireless communications system which could provide a given information transmission capacity, even in a very hostile environment (a signal/noise ratio much less than unit), if a corresponding frequency bandwidth (very large versus the information bandwidth) is used for transmission. For security reasons, the large frequency bandwidth had to be obtained by „spreading” the narrow bandwidth of information, using codes and modulations, which must be independent of information, which had to be known only by the transmitter and the intended receiver and this way, the last, in synchronism with the transmitter, could extract the information by correlation. Those codes became the „heart” and „signature” of CDMA, as they could differentiate the users and the networks,

allowing them to work in the same frequency band without interfering (multiple access) and „spreading” (rejecting) in the same time, all other (non-synchronized) signals.>>

From principles to the practical and tested solutions it is a very long way, as Claude Shannon, Irwin M. Jacobs (QUALCOMM founder) and other researchers proved and that is why the analyses have to be timely continued and include the changing context premises and evolutions.

Irwin M. Jacobs promoted SSS, also in the GSM standardization era, sometimes against all odds [1]. In fact, we believe [6] that Irwin M. Jacobs is, after theoretical founder Claude Shannon, another pillar of SSS evolution, this time mainly in the technical and technological areas, recognized by IEEE 2013 greatest award.

Even when ICT advanced with incredible progress for Large Scale Integration in the radio circuits, because of their complexity of implementation, SSS, along with provided incredible performances (antijam, anti-intercept features), were perceived with suspicion [1][6] and ***the word „complicated” was associated with CDMA and SSS.***

SSS were first intended and used only for military purposes (for example in strategic/priority applications, as military GPS, JTIDS/AWACS communications, mobile SINCGARS frequency hopping radios), but later, when the technological progress allowed it (in the late '80s), the civilian/commercial applications of SSS became possible, necessary and efficacious (SSS were first used only for communications and soon for radar, but later extended to GPS satellite, navigation etc.).

We have to recall that the ***SSS’s complicated concept, which was further developed long after Shannon’s theory, included, as a native/inherent feature, the CDMA.***

Irwin M. Jacobs received in 2013 the Medal of Honor from the Institute of Electrical and Electronics Engineers (IEEE), which is the highest honour an engineer can receive from his or her peers. The IEEE said he was receiving the award not just for his innovations but for "the ability to translate innovation into industry applications, time after time after time"[13].

We consider that recalling some details of Irwin M. Jacobs activity and results is twofold relevant:

- for the technical evolutions in a prominent/sensible area of modern communications;
- for understanding the potential of SSS/CDMA to leverage, along with AI, innovating models and algorithms which could be lend/used to mitigate the emergent security threats for our World or even for humankind knowledge refining and progress.

This opinion is at least partially confirmed by other references [1][13][6], where the highest level is represented by [1]:

<< “Someone else might have looked at all the complexities and the concerns and concluded that it just wasn't possible,” said Richard Atkinson, former president of the University of California. “But Irwin didn't back away.”

Making CDMA work was perhaps the easy part. Selling it to an industry already on the TDMA bandwagon was much tougher. The successful San Diego demonstration helped a lot, but it took years for CDMA to be truly accepted.>>

We also pointed with details the fascinating activity of Irwin M. Jacobs, just at the IEEE apogee recognition, in 2013 [6], as it follows:

<<This year, Irwin M. Jacobs received 2013 IEEE Medal of Honor for „leadership and fundamental contributions to digital communications and wireless technology”, as CDMA powers all 3G networks and is expanding its basics to 4G.

It is considered that Irwin M. Jacobs launched „a wireless revolution” [1].

Before leaving Massachusetts Institute of Technology (MIT), graduated by Jacobs after being a life-guard, a photo developer, a lumberjack and student at School of Hotel Administration

[1], (Irwin) „Jacobs and fellow faculty member John M. Wozencraft had written a textbook on communications theory, *Principles of Communication Engineering*, first published in 1965 and still used”. In 1966, after he earned a doctorate at MIT, he left for helping launch an engineering school in California, as professor at University of California, where he started a consulting company (Linkabit Corp), together with professors Andrew Viterbi and Leonard Kleinrock.>>

After these impressing “first” steps, Irwin M. Jacobs continued to reach incredible results [6][1]:

<<In 1985, Jacobs joined with six others, including Viterbi, he started QUALCOMM, a company which later had developed commercial CDMA and today is a leader in the world of communications (and generally ICT). One of the first contracts of QUALCOMM was with Hughes, to develop a mobile satellite system, where Hughes intended to use conventional spectrum-sharing techniques. In one of those days, in a car [1], in a pause between conversations with Andrew Viterbi and Klein Gilhousen, Irwin Jacobs thought that, in spite of the fact that CDMA were considered by other specialists „too complicated” for being used outside military applications (for commercial use), this technique could „squeeze” other users in the pauses between conversations of some users, as a multiple access in the same band.

That idea was the origin of the later epochal extension and evolution of CDMA in civilian applications, i.e. for cellular mobile communications.>>

More than presenting these evolutions, being implied in searching and promoting SSS in Romania, we observed, also in that 2013 paper, some strange, but surely scaled, coincidences reflecting SSS shocking features and specialist debate, even at considerable distances apart [6]:

<<In a similar way, keeping the scale, in 1979, when I have received the theme of the graduation paper at the Military Technical Academy (Bucharest) on „SSS communications”, everybody considered as „science fiction” the possibility to have wireless communications in the presence of a jamming with power of hundred times the useful signal power. Such opinions have persisted in 1981 when I have presented the first article on SSS at Politehnica University of Bucharest [11] and almost up to the publishing of the first books on SSS in Romania [5], [2].

It is worth to mention that SSS literature began to be public in a progressive manner, after 1982 when USA started their programme SINCGARS to develop tactical frequency hopping radios in the period 1982-1994 (aiming about 400 000 units in 1994).

In this context, the participation in 1992 at the first demonstrative exercise with tactical frequency hopping radios (Tadiran/SINCGARS- Bacau-Romania) and in 1995 at the Romanian Army’s auction for tactical frequency hopping radios (won by Racal-JAGUAR) and the SSS doctoral thesis in 1995 [7], represent moments of the evolution of SSS in Romania and in the same time results of what people’s knowledge and passion can do.>>

Irwin Jacobs and team fight had a long and fascinating evolution, against all odds and with essential results for modern communications [6][1]:

<<Knowledge and passion were the ingredients Irwin Jacobs (and Andrew Viterbi – the recipient of 2010 IEEE Medal of Honor) used to transform, after 1985, the CDMA extension idea into the actual mobile communications standards’ basics. That does not mean it was an easy way! Between 1985 and 1989, Jacobs and his QUALCOMM team, after showing the main advantages of CDMA for cellphones (higher number of users, better spectrum use, jam proofing communications) studied and solved „one of the biggest complexities” of CDMA: controlling the power of signals sent from the cellphone to the cell tower [1].

In 1989, when the first generation (G1) of mobile communications (MC) was in use as analogue technology, the principal producers decided to choose TDMA (time division multiple access) for the next generation of MC (G2), a digital technology, because they considered CDMA „too complicated” for G2. Despite of these opinions, Irwin Jacobs and QUALCOMM

continued the research and in november 1989 invited 100 producers or operators of cellphone systems at a CDMA demonstration, in San Diego. The demo was very dramatic: „if that demo had failed, we probably would have been died”, as Jacobs recalls [1].>>

Perhaps, sometimes, success and recognition have to be long and hardly expected, as fully was the case of Irwin Jacobs with CDMA [6][1]:

*<<As a matter of fact and strange coincidence, the two CDMA base stations had well operated, but they had used for synchronization (one of the most complicated problems of SSS and CDMA) the signals from then-nascent GPS (Global Positioning System) – a constellation of 24 satellites which today is the „natural” support for a huge diversity of mankind activities. For Jacobs’s desperation, the demo was blocked for 45 minutes, because in that period one of the GPS was itself out of synchronization. Notice GPS was using SSS/CDMA! Finally, the demo was an impressing success, but the CDMA way to industry was still long. In 1991, Jacobs and QUALCOMM had demonstrated CDMA for cellphone communications in New York, but the scepticism of wireless carriers executives still persisted. Very interesting is that, **at 1991 demo**, a Stanford professor „told people that CDMA violated the laws of physics” and The Wall Street Journal claimed in September 1996 that „Jacobs hype was causing carriers and cellphones manufacturers to throw away billions of dollars” [1].*

*As a strange coincidence (but great for Romania) is the fact that **10 years before**, when I have presented in 1981 my first paper on SSS, at Politehnica University of Bucharest [11], a very well-known communications professor, who wrote [12], said: „what this young guy has presented it’s impossible to work”.*

On the other hand, Jacobs and QUALCOMM continued and in July 1993 the Telecommunications Industry Association approved CDMA as standard. The first commercial CDMA network become operational in 1995 (Hong Kong) and QUALCOMM is today a 115 billion USD company [1]. >>

This way we could already think at using the SSS/CDMA ideas beyond ICT, in our World where **work ... without interfering (multiple access) ... in the same time** is an actual necessity everywhere on Earth.

Implementing and optimizing such ICT useful ideas in the complex context of our mentioned World challenges and crises is obviously a complicate and difficult process to be continued with refined knowledge, as changing paradigms or models is sometimes mandatory for sustainably innovating the progress.

2. Using AI to refine ICT solutions for mitigating everywhere the unexpected “interference” and cyber attacks

Watching the SSS evolutions and features we have observed only the start of a special combination of communications and AI, having a historical impact on radio communications, but also, beyond, on radar and further on ... World.

We could say that, from AI impact point of view, SSS opened a specific way of intelligent approach of signals structure and processing, used in radio communications and other areas, including radar and wide band data/computer networks [2][5][6].

This way, the amazing advances of ICT/AI continue to offer us new benefic surprises, especially in actual times when World challenges, crises and even chaotic turbulences seem to be impossible to mitigate. Here, AI began to provide, along with sometimes disputed hopes and results, interesting solutions also in the complex areas of „unexpected interferences”. To be more concrete, we should mention the huge progress of communications networks (2G, 3G, 4G, 5G) where AI role simply exploded.

Besides, AI advances are progressively imbedded in the new applications and systems which are developed along with ICT and communications services, in order to solve problems

with high or even unprecedented complexity/difficulty, which sometimes could appear as impossible, „unexpected” or even elusive interferences, without mentioning the huge area of challenges arisen from the defence, security, geopolitics or hybrid war realities of our turbulent World environment.

We think that this context and estimations could be better understood and quantified from the next relevant and comprehensive example, presented by [8]:

„Detection and mitigation of problem signals continue to evolve because of the following trends:

- 1. Continuous appearance of interferers as new communication services launch*
- 2. Proliferation of increasingly complex, difficult to detect signal events*
- 3. Challenge to stay at least one step ahead of potential interference problems*

... we explore these areas and delve into ways that spectrum monitoring and signal analysis techniques continue advancing to safeguard communications. A seemingly limitless variety of wireless systems operate in the world today, with new ones continuously emerging. Governments around the world do their best to regulate the electromagnetic (EM) spectrum, assigning specific frequency bands to certain communications applications. As these frequency bands become more crowded, networks are more likely to experience interference or even communications failure. These challenges arise from any radio-frequency (RF) system, including cellular phones and drones. These intentional or accidental signals can wreak havoc on a wireless system, creating issues such as noise in the channel or even loss of service. Spectrum monitoring continues to evolve to better detect and locate interferers in cellular and satellite communications while reinforcing key tactics to mitigate interference. In today’s crowded RF spectrum, interference is a frequent and unpredictable threat to performance and security. You need tools to help you detect, classify, and locate it quickly and accurately.”

It is important to notice the possible extrapolation of the above signal and interference issues, which inherently could be perceived from these lines, beyond the technical context and consequences, into all possible areas of actual World or human realities, considering ICT crucial role in IS toward KBS, as we already observed [21][18], which will be step by step more obvious here [8]:

“Finding the source of signal interference is difficult. The following are two different approaches to detecting signals: 1. RF sensors/fingerprinting. One method is to place time-synchronized RF sensors around the area of concern. A central control facility collects and analyzes data from these sensors. The software detects, identifies, and provides the location of interfering signals using a unique RF fingerprinting algorithm. Discovery of that fingerprint anywhere in the spectrum triggers geolocation, which leads to the emitter location. Imagine the shoreline of a lake; this process is much like measuring the ripples coming onshore in varying lengths after you throw a rock in the water. The sensors — gathering the information at the shoreline — can pinpoint where the rock hit the lake. 2. Handheld analyzer/geolocation software. Another step involves using a handheld analyzer in conjunction with the geolocation software. A geolocation algorithm can pinpoint the location of the interfering signal down to less than 100 meters, but you still need someone in that location with an instrument for those last few meters. A handheld analyzer with a directional wand antenna pointed in different directions will pick up the strongest signal. Determining the source of a moving signal, such as something transmitting from a vehicle, is a bit trickier. With continuous monitoring and geolocation, it is possible to determine the direction and speed of the moving signal. To identify a transmitter, you also can make a recording of it. A quadrature signal (IQ) recording gives you all the information

about that signal. You can leverage software to utilize that recording across various applications, driving it into different products. For example, signal analysis tools enable you to identify whether it is a signal appearing in the wrong band.”

Some special cases, of increasing interest in our days, for both security and civilian applications, include the *Drone Challenge* and *Hidden Signals*:

„Drones are increasingly popular as toys and for industrial uses. They pose threats in several different ways. As drones become cheaper, smaller, and more prevalent, someone can use them to observe a targeted location, carry drugs across a border, or even drop a dangerous substance onto a crowd or area. It is critical to be able to locate both the drone and the controller...Often, an interferer no longer appears when the equipment is set up to detect and locate it. Interferers are a common example of these elusive signals. They may affect communications — especially clarity or audibility of sound — by creating noise or distortion. Some signal events are elusive in a different way: they only occur occasionally. As the increasingly crowded spectrum results in more elusive signal events, new strategies are needed to detect, classify, locate, and mitigate interferers.”

It is useful to notice that, as the analysis is detailed, it reveals more complicated/difficult problems, as ICT advances and in this case, it is necessary to know *how signals hide*:

“If a system and the interferer are on the same frequency, nothing appears wrong on a spectrum analyser. The two signals appear right on top of each other, like one normal signal. Yet interference often reveals itself by affecting audibility and clarity via noise or distortion. Other signal events are elusive because they rarely occur, maybe once a month or year. Yet they still can cause significant problems, depending on their frequency. Even if an interfering signal event occurs only once a year, it could negatively affect mission-critical systems like emergency services or early-warning systems. From traditional swept heterodyne methods to sensors and fast Fourier transform (FFT) approaches, evolving spectrum monitoring methods more effectively detect, identify, and report on these hard-to-find signals to ensure better communications.”

As a consequence, also the approach solutions have to be refined, in order to optimize the chances and efficiency of success:

<<To maintain awareness of elusive or problem signals, engineers looking to perform spectrum monitoring follow one of two approaches: survey or search. With the first method, the engineer surveys the spectrum to determine what signals occur in an environment. The engineer can then create a table of frequencies, bandwidths, and modulation types. Those coming to a new area to erect a tower use this “spectral survey”. The second approach — search — is trickier. Here, the engineer usually watches a specific signal because of information that is already known. For example, who is the owner or who is using it? The search could focus on an individual’s cell phone number or devices in use. The user or agency performing the search preloads that information into a system and tells the system to find those elements. If the system detects that signal, it sends an immediate notification>>

Here, between the lines, we can observe that, along with engineers expertise, the AI power and data base are essential to find the “documented” elusive signal event:

“To detect and identify an elusive signal, begin with the environmental scan or survey to determine what signals are in the environment. Frequently, engineers have already documented the signals they are broadcasting or using and know which channels are effective versus the ones that exhibit issues. Problems usually show up in a specific frequency or channel. You can use that information to focus your survey on that area of the spectrum. With a spectrum analyser, you may not see the interfering signal if it is riding right on top of the signal for which you are searching. When everything appears fine, but performance issues clearly exist, the next step is to deploy sensors around the area. By placing four or five sensors

a mile or so apart, for example, you can perform the same survey again in that frequency band.”

Finally, it is clear that the complexity of such searching and monitoring, the spectrum or other similar assets/contexts, needs a continuous activity, including AI/software, but improving it as the context and technology are changing and we have to “*prepare for the future*”:

“No matter the approach, spectrum monitoring is a critical aspect of safeguarding spectrum and communications systems. More organizations now opt for ongoing spectrum monitoring rather than just bringing in such capabilities when problems arise. Spectrum monitoring software automates signal search and survey functions.”

Going further with AI help, in our full of uncertainties World, today we have to be prepared for any kind of „interference”, i.e., beyond electromagnetic spectrum issues, now we could notice also some encouraging advances in the extremely complicated area of cyber security, as it could be observed from [10]:

“Recently, deep learning and neural networks (NNs) have demonstrated exceptional performances in many areas, including image recognition, robotics, and natural language processing. Compared to traditional machine learning models (for example, decision trees (DTs), random forests, support vector machines, and so on), NNs have notable advantages including the abilities of dealing with complex data, reduced reliance on feature extraction, comparatively better performances, and so on. However, due to the black-box nature of NNs, understanding how models make decisions is often difficult, both in a general sense (explanation) and in the context of a specific input (interpretation). This has hindered the applications of NNs in some critical missions where understanding rationales of the decision-making is imperative. This is especially true in the security domain. System administrators want to not only determine if the system is under attack but also identify what indicators signal the potential attack, as the indicators are often the cues for knowing the root causes.”

Although here it is another area, different of spectrum, we observe, from the beginning and perhaps more than above, that the optimization solution is much complicate and especially difficult to certainly find and interpret in order to decide which is the cause/author:

<<For example, an NN-based network intrusion detection system (NIDS) usually detects intrusions including denial of service, probing, botnet, and other logic flaw exploiting attacks. It can take network packets or postprocessing network data (for example, network flow data) as input and report whether (specific kinds of) attacks exist. If a NN-based NIDS detects an attack, the security analyst will want to know which packets lead to the attack, where the attack packets come from, and sometimes even which bytes of the packets are malicious. To achieve this goal, explainable artificial intelligence (XAI) is a valuable tool that can be used to “crack open the black box.”>>

In fact, we have to agree that the search of unexpected threats between billions of bits, from billions of sources/persons, sometimes in real time, is a kind of nightmare and consequently needs to analyse and weight many variables:

“One of the XAI techniques that have been tailored to cybersecurity problems with domain-specific knowledge is Trustee. It learned high-fidelity and low-complexity DTs for network security problems. The DT is easy to interpret and can be used to identify the most important features for making predictions, as well as to understand the decision-making process used by the model. Humans can comprehend and retrace how AI models came to a specific output based on the DTs. However, DTs also have some limitations when used for explaining black-box deep learning models. For example, DTs may not be able to capture complex relationships between input features, and they may be sensitive to noise and outliers in the data. Therefore, it is important to carefully evaluate the use of DTs for explaining

AI models used in network security. For example, DTs may not be able to capture complex relationships between input features, and they may be sensitive to noise and outliers in the data”.

It is important to notice that, for maximal trust and clarity of decisions, the human intelligence (HI) is again the key factor and the *experts’ domain knowledge* is necessary:

<<Shapley values produced by SHAP, a widely used tool to provide per-data sample explanations, are used for measuring the impact of a certain feature’s value toward the predicted result. Different from TRUSTEE, Shapley values are used for local interpretation. In other words, it is used to interpret how a prediction result is reached for a specific data sample. Specifically, Shapley values can tell how each feature contributes to the predicted results. Since the explanations provided by DTs and SHAP are two different kinds of explanations, we believe that no meaningful conclusions on “which explanations are better” could be drawn. However, we observe that from the perspective of whether the explanations are in agreement with the experts’ domain knowledge, the explanations provided by both DTs and SHAP are actually located on the same spectrum.>>

Our opinion and the main conclusion are that, using all power and progress of AI, the human intelligence must remain the main reference for such mission critical applications and AI development, advance and use [16][22].

In spite of the visible complexity and promising results of ICT/AI, we can see how complicate is the fight with unexpected interference or cyber attacks and consequently how “long and winding road” must be done, even with the fast AI advances which are, of course, the expected solutions where the complexity and Big Data are more and more present, but it is **worth to notice the HI which “support” both sides of the competition.**

After such deep issues of AI potential, which we consider, one more time [19][18], only a tip of the iceberg, we could agree that ICT, communications and generally humankind should benefit from AI advances, having the updated HI and refined knowledge inside, in a “large spectrum” of approaches, as SSS and CDMA already proved to be a start.

It is sure that only human imagination and refined knowledge could limit, in our actual and future turbulent World, what the mentioned “large spectrum” could mean, or understanding what could be behind generic “interference” and “malicious bits”, but we believe that **some ingredients of such approaches could be still seen from the technical features of SSS and CDMA example.**

On this way, coming back to our paper aim, it is interesting to recall that, even from 2013, we observed the relevance of ICT/SSS advances for the emerging World challenges [6]:

<<One of the fascinating mechanisms of ICT exponential development is the power of its innovations to multiply their effects not only in the technological world, but also in the human society they build as IS, by a diversity of consequences, mainly linked with the people’s minds. In the reality, the IS development, even it is based on ICT growing, would not be possible if ICT would not have such a complex and dramatic mutual dependence with the mankind creation capacity. If we try to find the beginning of this „circle”, we surely must admit that always the man is first, i.e., understand how important the knowledge, the innovation and the human passion are, for the achievement of such huge and complicated things, as CDMA/SSS is... Here we would like to reveal the particular ways CDMA, as a prominent concept of actual ICT, could help people’s creation processes. As we already presented in the Network Centric and Cloud cases [9], CDMA is also a model that could influence IS beyond the obvious ways of the ICT technological implications, even if the CDMA influence were not in the same ways and dimensions. The essential observation could be extracted just from the Irwin Jacobs’s initial idea: we can optimize a process by reusing the pauses, i.e., the time.>>

Here we have to add the role of “refined knowledge inside”, which could not be separated of education processes, in IS/KBS:

<<We also have mentioned [9] that one of the ICT essential contributions to the people's education and to IS is given by the products and services which enable the people to reuse the time and generally to optimize the use of time with an amazing efficiency. If we would try again to simply express the „too complicated” CDMA, we have to observe that the novelty CDMA brings, versus the conventional multiple access techniques (TDMA- time division multiple access; FDMA=frequency division multiple access), consists of optimizing both time and frequency, in a sophisticated manner: by assigning to users and networks special codes, which may be simpler (shorter and easy generated) or very complicated (longer, if necessary highly and multi-criteria elaborated), depending of application's desired performances.

As another strange coincidence, we achieved [7] by extending Gold codes generating techniques and proposing a new similar class of codes for CDMA/SSS [4]. And how? By refining mathematical knowledge (Galois Extended Fields), work, passion and ... Personal Computers.

Coming back to people, **CDMA could teach us to optimize time and other resources** (not only frequency spectrum), by refining (coding=linking in new ways) the knowledge, i.e., innovating the ways we used to think, we used to do anything, we used to work, we used to consume, we used to learn, we used to imagine and so on. In all the above examples, using the CDMA's model, the people could learn, without restricting their rights, that in the more and more „complicated” life on Earth, we have to refine our knowledge using the latest information, we have to innovate new ways to improve or at least to preserve all the Earth and mankind resources.>>

More than these obvious issues, we could observe, after 10 years of World “progress”, not only the right direction, but also **the painful actuality**, opportunity and even the necessary holistic approach of all useful factors/resources to mitigate/combat the aggressive World challenges we have to face today and tomorrow:

<<We have also to adapt and face the new challenges of life, including the „side effects” of the technological progress, using the CDMA/SSS models, which „compute” and provide any „slice” of **all the resources** for every user and network, in a precise and negotiated order, avoiding interference and conflicts. Perhaps the simplest form to concentrate the paper's essence is to emphasize the power of CDMA to leverage the mankind activity, by technological concrete consequences and also as a model to manage the resources - from time and electromagnetic spectrum to anything people must share on Earth.

A subsequent lesson people could learn from CDMA is to better and wiser live with the neighbours and environment, reducing the „mutual interference” and being more tolerant on a rational (coded=calculated/rational) basis. The „secure” feature of CDMA/SSS could help us to respect privacy and personal information, such idea being very actual as social networks already reveal their risks on privacy and overdoing.

In the same field of Internet and beyond (in IS) we may see the danger of governments tendencies to interfere with the private life and information, without speaking of similar international political actions, state cyber-attacks etc.

Finally, we may come back with an optimistic observation: **against all of these „attacks”, CDMA/SSS could defend and support us in concrete ways, based on standards which include CDMA/SSS, as IEEE 802.xx family (which includes WiFi, Bluetooth, WiMax) and the universal cellphone networks 3G and 4G and... beyond.>>**

Beyond the transparence of the presented technical features (anti interference, anti cyber attacks etc.) to rational hints about the generic interferences/attacks at the human essential struggle for survival, we should understand, still, the potential of ICT/AI and HI to support our World against the seen and even unexpected threats, which could be optimally used only by spreading the necessary “refined knowledge inside”, before the threats advance and before... being too late! But we have to not forget to imagine and be

prepared, what if Internet, communications or AI does not work, at least partially, for a while...one day, as some interferences/incidents already showed!

3. Conclusions

The actual World crises and challenges generate unprecedented levels of concern for most people and incumbents, just reminding the recent aggressive consequences of global warming (climate changes), but also the progressive Earth resources fading, social unbalances or geopolitical/security crises, threats against democracy or changes in human behaviour/habit values [16][19][15][17][18][23]. **This worrying complex context is the reason why we considered useful (and actual!) to recall some historical evolutions of ICT and communications, including even relative recent ones from our paper [6], just to emphasize the amazing speed of World colliding crises and then the necessity to learn from history and use all the resources for surviving.** Also, recently [14], we observed, one more time, **some indirect ways the ICT could leverage the World progress and mitigate the above challenges, by deeply innovating its advances.** One way ICT could contribute to this World fight/progress is an indirectly one, recalling that its proven efficient/automated models and algorithms of development and proliferation could be largely used/lend to other fields of human activity [22].

As our World complex, complicate and fast changing context we are in could be, sometimes, perceived and studied as a result of cumulating/interfering factors, including some of them unknown, unexpected or undefined (*like social media underground influence on person behaviour*), the paper analysis is intended to reveal some ICT ways/solutions for interference (as general meaning) mitigation, including communications and artificial intelligence (AI) advanced results, while the possibilities to use these approaches in other areas are relevant. Our opinion is that, analysing some models/technologies of the ways ICT and the communications equipments/networks fight interference is not only a useful technical example of ICT innovation/progress, but also an inspiration and even instrument for the complex and difficult approach of other similar World and humankind emerging challenges.

It is useful to shortly recall some basic or historical moments of communications equipments/networks (and generally of ICT), where solutions to mitigate interference and other vulnerabilities were in focus, as the aim of this paper is not only to show the role of such historical moments, from the point of view of science and technology evolutions, but mainly to reveal the context models (including AI) which could be beneficently extended to other World challenges, emergent or foreseen, where “unexpected interference”, as a generic, but not necessary technical concept, could be a threat, as lately, in our World of crises, we have encountered, especially through social media (like TikTok) or other kinds of cyber-attacks or hybrid war.

The subject of „interference resistance” was presented in a new approach [3] and we think that adding some details to this context could be interesting and useful for the paper mentioned aim about the communications development.

Communications development, while providing more and more benefits, keeps a so called “Achile’s heal” vulnerability, by the fact that any communication, especially for defence and security purposes, could inherently offer to the enemy, or to the third party, some information, at least by the simple using or radiation of energy, which is more than obvious in the case of radiocommunications. Even in the non-military applications, the sensitivity or susceptibility to electromagnetic interference is also an important vulnerability to be technically approached and mitigated, i.e., the analysis and the eventual solutions are important and of general interest, from the point of view of electromagnetic compatibility.

The protection of military radio communications, from their early moments, led to the first ideas to avoid interference or information interception, about the time of World War I, although, much later, a diversity of patents was claimed, one of them getting additional benefit due to a famous actress. We analysed the case of *Actress Hedy Lamarr, who co-patented a widely used secure communication technology, having partner the radical modernist composer George Antheil* [3], but it is also confirmed that the dutch inventor Willem Broertjes, on October 11, 1929, submitted a patent application in Germany for a “*Method of Maintaining Secrecy in the Transmission of Wireless Telegraph Messages.*” A month later Broertjes filed an application in America, and in 1932 he was awarded U.S. Patent 1,869,659, where it clearly expressed the essence (***a periodically modified transmission frequency, which is received by means of a receiving apparatus, the tuning of which is modified in synchronism***).

More than the significance of these examples, we consider that the reality, about the spread spectrum systems (SSS) in general, is much more complex and fuller of scientific and technical relevant details, we also researched, with some national level results [7][2][27], while we have introduced them in the university teaching process in the Military Technical Academy [5][28][29][30]. The specialists mainly recognize that the scientific basics of communications with SSS, after some steps of patents evolution, were mainly given, in 1945, by Claude Shannon formula/equation of channel capacity and on the other hand the technical definitional requirements of SSS could be essentially expressed by 2 requirements and some performance features [26][24][25][2][27], including (the multiplicity factor $\gg 1$) and PN spreading law, along with features like anti-jam, LPI, CDMA and (DS, FH, TH) spreading techniques. The key factor of secret and reliable synchronization between receiver and transmitter is the most complex and difficult part, especially for getting antijam, anti-intercept features, which is not the case of non-military applications [26][2][5][27]. Still, much of non-military applications, as CDMA and FH (including but not limiting to Bluetooth, WiFi, WiMax or OFDM), expanded in almost all modern communications, including 2G to 5G networks, do not truly (maximally) respect/provide the above-mentioned definitional requirements of SSS and consequently the performances.

We also analysed the requirements and some performance features of SSS, with some technical details, given yet from [6], where „spreading” codes and modulations (CDMA), synchronism and correlation were pointed, while *those codes became the „heart” and „signature” of CDMA, as they could differentiate the users and the networks, allowing them to work in the same frequency band without interfering (multiple access) and „spreading” (rejecting) in the same time, all other (non-synchronized) signals.*

Still, from principles to the practical and tested solutions it is a very long way, as Claude Shannon, Irwin M. Jacobs (QUALCOMM founder) and other researchers proved (Irwin M. Jacobs promoted SSS, also in the GSM standardization era, sometimes against all odds [1]). In fact, we believe, [6], that Irwin M. Jacobs is, after the theoretical founder Claude Shannon, another pillar of SSS evolution, this time mainly in the technical and technological areas, recognized by IEEE 2013 greatest award. Even when ICT advanced with incredible progress for Large Scale Integration in the radio circuits, because of their complexity of implementation, SSS, along with provided incredible performances (antijam, anti-intercept features), were perceived with suspicion [1][6] and ***the word „complicated” was associated with CDMA and SSS.***

We also pointed with details the fascinating activity of Irwin M. Jacobs, just at the IEEE apogee recognition, in 2013 [6], as it follows: <<...***It is considered that Irwin M. Jacobs launched „a wireless revolution”*** [1]. In 1985, Jacobs joined with six others, including Viterbi, he started QUALCOMM, a company which later had developed commercial CDMA and today is a leader in the world of communications (and generally ICT)...In one of those days, in a car [1], in a pause between conversations with Andrew Viterbi and Klein Gilhousen,

Irwin Jacobs thought that, in spite of the fact that CDMA were considered by other specialists „too complicated” for being used outside military applications (for commercial use), this technique could „squeeze” other users in the pauses between conversations of some users, as a multiple access in the same band. **That idea was the origin of the later epochal extension and evolution of CDMA in civilian applications, i.e. for cellular mobile communications>>.**

More than presenting these evolutions, being implied in searching and promoting SSS in Romania, we observed, also in that 2013 paper, some strange, but surely scaled, coincidences reflecting SSS shocking features and specialist debate, even at considerable distances apart [6] <<In a similar way, keeping the scale, in 1979, when I have received the theme of the graduation paper at the Military Technical Academy (Bucharest) on „SSS communications”, everybody considered as „science fiction” the possibility to have wireless communications in the presence of a jamming with power of hundred times the useful signal power. Such opinions have persisted in 1981 when I have presented the first article on SSS at Politehnica University of Bucharest [11] and almost up to the publishing of the first books on SSS in Romania [5], [2]... SSS literature began to be public in a progressive manner, after 1982 when USA started their programme SINGARS to develop tactical frequency hopping radios in the period 1982-1994 (aiming about 400 000 units in 1994)... participation in 1992 at the first demonstrative exercise with tactical frequency hopping radios (Tadiran/SINGARS- Bacau-Romania) and in 1995 at the Romanian Army’s auction for tactical frequency hopping radios (won by Racal-JAGUAR) and the SSS doctoral thesis in 1995 [7], represent moments of the evolution of SSS in Romania and in the same time results of what people’s knowledge and passion can do>>.

Further, Irwin Jacobs and team fight had a long and fascinating evolution, against all odds and with essential results for modern communications [6][1]: << In 1989, when the first generation (G1) of mobile communications (MC) was in use as analogue technology, the principal producers decided to choose TDMA (time division multiple access) for the next generation of MC (G2), a digital technology, because they considered CDMA „too complicated” for G2. Despite of these opinions, Irwin Jacobs and QUALCOMM continued the research and in november 1989 invited 100 producers or operators of cellphone systems at a CDMA demonstration, in San Diego. The demo was very dramatic: „if that demo had failed, we probably would have been died”, as Jacobs recalls [1]>>.

Sometimes, success and recognition have to be long and hardly expected, as fully was the case of Irwin Jacobs with CDMA[6][1]: <<As a matter of fact and strange coincidence, the two CDMA base stations had well operated, but they had used for synchronization (one of the most complicated problems of SSS and CDMA) the signals from then-nascent GPS (Global Positioning System) – a constellation of 24 satellites which today is the „natural” support for a huge diversity of mankind activities... the demo was blocked for 45 minutes, because in that period one of the GPS was itself out of synchronization. Notice GPS was using SSS/CDMA! Finally, the demo was an impressing success, but the CDMA way to industry was still long. In 1991, Jacobs and QUALCOMM had demonstrated CDMA for cellphone communications in New York, but the scepticism of wireless carriers executives still persisted. Very interesting is that, **at 1991 demo**, a Stanford professor „told people that CDMA violated the laws of physics” and The Wall Street Journal claimed in September 1996 that „Jacobs hype was causing carriers and cellphones manufacturers to throw away billions of dollars”[1]. As a strange coincidence (but great for Romania) is the fact that **10 years before**, when I have presented in 1981 my first paper on SSS, at Politehnica University of Bucharest [11], a very well known communications professor, who wrote [12], said: „what this young guy has presented it’s impossible to work”. On the other hand, Jacobs and QUALCOMM continued and in July 1993 the Telecommunications Industry Association approved CDMA as standard. The first commercial CDMA network become operational in 1995 (Hong Kong) and QUALCOMM is today a 115 billion USD company [1] >>.

We could think at using the SSS/CDMA ideas beyond ICT, in our World where *work without interfering (multiple access) ... in the same time* is an actual necessity everywhere on Earth, but, **implementing and optimizing such ICT useful ideas in the complex context of our mentioned World challenges and crises is obviously a complicate and difficult process to be continued with refined knowledge, as changing paradigms or models is sometimes mandatory for sustainably innovating the progress.**

The above SSS evolutions and features, we have observed, are only the start of a special combination of communications and AI, having a historical impact on radio communications, but also, beyond, on radar and further on ... World. **From the AI impact point of view, SSS opened a specific way of intelligent approach of signals structure and processing, used in radio communications and other areas, including radar and wide band data/computer networks [2][5][6].** The amazing advances of ICT/AI continue to offer us new benefic surprises, especially in actual times when World challenges, crises and even chaotic turbulences seem to be impossible to mitigate. AI began to provide, along with sometimes disputed hopes and results, interesting solutions also in the complex areas of „unexpected interferences”. To be more concrete, we should mention the huge progress of communications networks (2G, 3G, 4G, 5G) where AI role simply exploded.

AI advances are progressively imbedded in the new applications and systems which are developed along with ICT and communications services, in order to solve problems with high or even unprecedented complexity/difficulty, which sometimes could appear as impossible, „unexpected” or even elusive interferences, without mentioning the huge area of challenges arisen from the defence, security, geopolitics or hybrid war realities of our turbulent World environment. This context and estimations could be better understood and quantified after the analysis of a relevant and comprehensive example, presented by[8], about *spectrum monitoring and signal analysis techniques, as a limitless variety of wireless systems operate in the world today, and governments around the world do their best to regulate the electromagnetic (EM) spectrum...Spectrum monitoring continues to evolve to better detect and locate interferers in cellular and satellite communications while reinforcing key tactics to mitigate interference.* We noticed the possible extrapolation of the above signal and interference issues, which inherently could be perceived from these lines, beyond the technical context and consequences, into all possible areas of actual World or human realities. *The software detects, identifies, and provides the location of interfering signals using a unique RF fingerprinting algorithm. Discovery of that fingerprint anywhere in the spectrum triggers geolocation, which leads to the emitter location.* Some special cases, of increasing interest in our days, for both security and civilian applications, include the *Drone Challenge* and *Hidden Signals*. It is useful to notice that, as the analysis is detailed, it reveals more complicate/difficult problems, as ICT advances, in this case it is necessary to know *how signals hide*. Between the lines, we observed that, along with engineers expertise, the AI power and data base are essential to find the “*documented*” *elusive signal event*. Finally, it is clear that the complexity of such searching and monitoring, the spectrum or other similar assets/contexts, needs a continuous activity, including AI/software, but improving it as the context and technology are changing and we have to “*prepare for the future*”:

Going further with AI help, in our full of uncertainties World, today we have to be prepared for any kind of „interference”, i.e., beyond electromagnetic spectrum issues. Now we could notice also some encouraging advances in the extremely complicated area of cyber security, as it was analysed from [10], where *deep learning and neural networks (NNs) have demonstrated exceptional performances in many areas, including image recognition, robotics, and natural language processing...* Here it is another area, different of spectrum and we observe that the optimization solution is much complicate and especially difficult to certainly find and interpret in order to decide which is the cause/author: *If a NN-based NIDS detects an*

attack, the security analyst will want to know which packets lead to the attack, where the attack packets come from, and sometimes even which bytes of the packets are malicious. In fact, we have to agree that the search of unexpected threats between billions of bits, from billions of sources/persons, sometimes in real time, is a kind of nightmare and consequently needs to analyse and weight many variables: *“One of the XAI techniques that have been tailored to cybersecurity problems with domain-specific knowledge is Trustee. It learned high-fidelity and low-complexity DTs for network security problems... For example, DTs may not be able to capture complex relationships between input features, and they may be sensitive to noise and outliers in the data”*. It is important to notice that, for maximal trust and clarity of decisions, the HI is again the key factor and the *experts’ domain knowledge* is necessary: *„However, we observe that from the perspective of whether the explanations are in agreement with the experts’ domain knowledge, the explanations provided by both DTs and SHAP are actually located on the same spectrum”*.

Our main conclusion is that, using all power and progress of AI, the human intelligence must remain the main reference for such mission critical applications and AI development, advance and use [16][22].

In spite of the visible complexity and promising results of ICT/AI, we can see how complicate is the fight with unexpected interference or cyber attacks and consequently how “long and winding road” must be done, even with the fast AI advances which are, of course, the expected solutions where the complexity and Big Data are more and more present, but it **is worth to notice the HI which “support” both sides of the competition**.

After such deep issues of AI potential, which we consider, one more time [19][18], only a tip of the iceberg, we could agree that ICT, communications and generally humankind should benefit from AI advances, having the updated HI and refined knowledge inside, in a “large spectrum” of approaches, as SSS and CDMA already proved to be a start.

It is sure that only human imagination and refined knowledge could limit, in our actual and future turbulent World, what the mentioned “large spectrum” could mean, or understanding what could be behind generic “interference” and “malicious bits”, but we believe that **some ingredients of such approaches could be still seen from the technical features of SSS and CDMA example**. On this way, coming back to our paper aim, it is interesting to recall that, even from 2013, we observed the relevance of ICT/SSS advances for the emerging World challenges [6]: *<<CDMA is also a model that could influence IS beyond the obvious ways of the ICT technological implications, even if the CDMA influence were not in the same ways and dimensions. The essential observation could be extracted just from the Irwin Jacobs’s initial idea: we can optimize a process by reusing the pauses, i.e., the time>>*.

We also have to point the role of “refined knowledge inside”, which could not be separated of education processes, in IS/KBS: *<<We also have mentioned [9] that one of the ICT essential contributions to the people’s education and to IS is given by the products and services which enable the people to reuse the time and generally to optimize the use of time with an amazing efficiency. If we would try again to simply express the „too complicated” CDMA, we have to observe that the novelty CDMA brings, versus the conventional multiple access techniques (TDMA...FDMA), consists of optimizing both time and frequency, in a sophisticated manner: by assigning to users and networks special codes, which may be simpler (shorter and easy generated) or very complicated (longer, if necessary, highly and multi-criteria elaborated), depending of application’s desired performances. As another strange coincidence, we achieved [7] by extending Gold codes generating techniques and proposing a new similar class of codes for CDMA/SSS [4]. And how? By refining mathematical knowledge (Galois Extended Fields), work, passion and ... Personal Computers. Coming back to people, CDMA could teach us to optimize time and other resources (not only frequency spectrum), by refining ... the knowledge, i.e., innovating the ways we used to think, we used to do anything,*

we used to work, we used to consume, we used to learn, we used to imagine and so on. In all the above examples, using the CDMA's model, the people could learn, without restricting their rights, that in the more and more „complicated” life on Earth, we have to refine our knowledge using the latest information, we have to innovate new ways to improve or at least to preserve all the Earth and mankind resources>>.

We could observe, after 10 years of World “progress”, not only the right direction, but also **the painful actuality**, opportunity and even the necessary holistic approach of all useful factors/resources to mitigate/combat the aggressive World challenges we have to face today and tomorrow: *<<We have also to adapt and face the new challenges of life, including the „side effects” of the technological progress, using the CDMA/SSS models, which „compute” and provide any „slice” of **all the resources** for every user and network, in a precise and negotiated order, avoiding interference and conflicts... emphasize the power of CDMA to leverage the mankind activity, by technological concrete consequences and also as a model to manage the resources - from time and electromagnetic spectrum to anything people must share on Earth. A subsequent lesson people could learn from CDMA is to better and wiser live with the neighbours and environment, reducing the „mutual interference” and being more tolerant on a rational (...calculated/rational) basis. The „secure” feature of CDMA/SSS could help us to respect privacy and personal information, such idea being very actual as social networks already reveal their risks on privacy and overdoing. In the same field of Internet and beyond (in IS) we may see the danger of governments tendencies to interfere with the private life and information, without speaking of similar international political actions, state cyber-attacks etc. Finally, we may come back with an optimistic observation: **against all of these „attacks”, CDMA/SSS could defend and support us in concrete ways, based on standards which include CDMA/SSS, as IEEE 802.xx family (which includes WiFi, Bluetooth, WiMax) and the universal cellphone networks 3G and 4G and... beyond>>.***

Beyond the transparence of the presented technical features (anti interference, anti cyber attacks etc.) to rational hints about the generic interferences/attacks at the human essential struggle for survival, we should understand, still, the potential of ICT/AI and HI to support our World against the seen and even unexpected threats, which could be optimally used only by spreading the necessary “refined knowledge inside”, before the threats advance and before... being too late! But we have to not forget to imagine and be prepared, what if Internet, communications or AI does not work, at least partially, for a while...one day, as some interferences/incidents already showed!

REFERENCES

- [1]Tekla S. Perry, *Captain Cellular*, IEEE Spectrum, May 2013.
- [2]Victor P. Greu, *Jamming and Interference resistant radio communications*, The Military Printing House, Bucharest, 1992 (in Romanian language).
- [3]Tony Rothman, *Random Paths to Frequency Hopping*, American Scientist, January-February 2019, Volume 107, Number 1, <https://www.americanscientist.org/article/random-paths-to-frequency-hopping>
- [4]Victor Greu, Bogdan Vasilescu, *Basic method for generating "quasi-orthogonal" spread-spectrum signal formats*, Proceedings of the International Conference "ECCTD'97(European Conference on Circuits Theory and Design)", Budapest-Hungary, 1997.
- [5]Victor Greu, *Spread Spectrum Communications Systems*, The Military Technical Academy Printing House, Bucharest, 1997 (in Romanian language).
- [6]Victor Greu, *The Code Division Multiple Access from Complicated to The Actual Mobile Communications Standards and Beyond*, Romanian Distribution Committee Magazine, Volume 4, Issue 3, Year 2013.

- [7]Victor P. Greu, *Methods to realize the spread-spectrum communications systems (Doctoral Thesis)*, The Military Technical Academy, Bucharest, 1995 (in Romanian language).
- [8]***, *A Practical Guide to Locate and Mitigate Interference eBook*, © Keysight Technologies, 2020 – 2023, Published in USA, March 13, 2023
- [9]Victor Greu, *The Network Centric and Cloud - A New Paradigm for The Optimization of The Technical and Human Information Systems*, Romanian Distribution Committee Magazine, Volume 2, Issue 2, Year 2011.
- [10]Qingtian Zou, Lan Zhang, Xiaoyan Sun, Anoop Singhal, Peng Liu, *Using Explainable AI for Neural Network-Based Network Attack Detection*, Computer, Volume 57, Issue 5, 02 May 2024, <https://doi.org/10.1109/MC.2023.3342602>
- [11]Victor Greu, *Interference Stable Spread-Spectrum Information Transmission Techniques*, Presented at The Jubilee Conference „100 years of engineering higher education in Romania”, Politehnica University of Bucharest, 1981 (in Romanian language).
- [12]Mugur Savescu, *Radio relays and spatial radio communications, Pedagogical and didactic Printing House, Bucharest, 1976* (in Romanian language).
- [13]Freeman Mike, *Qualcomm founder Jacobs gets IEEE award*, San Diego Union Tribune, Retrieved August 20, 2013
- [14]Victor Greu, *Improving information and communication technology to innovate the paradigms of World progress-(Part 1)*, Romanian Distribution Committee (affiliated to the “International Association of the Distributive Trade”-scientific association – A.I.D.A. Brussels) Magazine(international; electronic; covered in RePEc International Data Base), Volume 15, Issue 1, Year 2024.
- [15]***, *Strategies to Tackle Uncertainty With AI Deployment*, Computer Society Team, 12/19/2022, <https://www.computer.org/publications/tech-news/research/strategies-to-tackle-uncertainty-with-ai-deployment>
- [16]Victor Greu, *Searching the right tracks of new technologies in the earth race for a balance between progress and survival*, Romanian Distribution Committee (affiliated to the “International Association of the Distributive Trade”-scientific association – A.I.D.A. Brussels) Magazine(international; electronic; covered in RePEc International Data Base), Volume 3, Issue1, Year 2012.
- [17]Giuliano Punzo et al, *Engineering Resilient Complex Systems: The Necessary Shift Toward Complexity Science*, IEEE SYSTEMS JOURNAL, VOL. 14, NO. 3, SEPTEMBER 2020
- [18]Victor Greu, *Information and communications technology is merging data science and advanced artificial intelligence towards the core of knowledge based society -(Part 3)*, Romanian Distribution Committee (affiliated to the “International Association of the Distributive Trade”-scientific association – A.I.D.A. Brussels) Magazine(international; electronic; covered in RePEc International Data Base), Volume 12, Issue 3, Year 2021.
- [19]Victor Greu, *Information and communications technologies go greener beyond IOT-behind is all the earth-Part1*, Romanian Distribution Committee (affiliated to the “International Association of the Distributive Trade”-scientific association – A.I.D.A. Brussels) Magazine(international; electronic; covered in RePEc International Data Base), Volume 7, Issue 2, Year 2016.
- [20]Gareth Smith, *Demystifying intelligent automation*, May 2022, <https://www.enterpriseitworld.com/demystifying-intelligent-automation-2/>
- [21]Victor Greu, *The information and communications technology is driving artificial intelligence to leverage refined knowledge for the World sustainable development – (Part 2)*, Romanian Distribution Committee (affiliated to the “International Association of the Distributive Trade”-scientific association – A.I.D.A. Brussels) Magazine(international; electronic; covered in RePEc International Data Base), Volume 10, Issue 1, Year 2019.

- [22]Florin Enache, Victor Greu, Petrică Ciotîrnae, Florin Popescu, *Model and Algorithms for Optimizing a Human Computing System Oriented to Knowledge Extraction by Use of Crowdsourcing*, 2020, 13th International Conference on Communications (COMM), (Politehnica University of Bucharest, Military Technical Academy, IEEE Romania), (COMM 2020 is covered in IEEE Explore Database and ISI Web of Science in the Conference Proceedings Citation Index)
- [23]Kathy Pretz, *IEEE Discusses 6 Simple Solutions to Climate Change at COP27*, IEEE Spectrum -The Institute, Jan 2023, https://spectrum.ieee.org/6-solutions-to-climate-change?utm_source=feedotter&utm_medium=email&utm_campaign=theinstitutealert-020723&mkt_tok=NzU2LUdQSC04OTkAAAGJydzxSHpuq5OM3DCG1vf09lo7cS9SF4diBorTarLno1KsPH--DxoBUdWtSI7n1JnvJ-xzsuSpD5nTSp4emRYFU-PhQVmcqj5VigYPQwsBCo
- [24]Scholtz R. A. , *The origins of spread spectrum communications*. IEEE Communications Transactions, May 1982
- [25]Simon M. K., J. K. Omura, R. A. Scholtz, and B. K. Levitt, *The Spread Spectrum Communications Handbook*, 1994, New York: McGraw-Hill.
- [26]Dixon R.C., *Spread Spectrum Systems*, Published by Wiley-Interscience, 1976
- [27]Victor Greu, Constantin Mincu, Costel Rotariu, *Frequency Hopping and Counter Frequency Hopping*, The Military Printing House, Bucharest, 1997 (in Romanian language).
- [28]Victor Greu, Dorin Andrei, *Spread Spectrum Communications Systems for Electronic and Informational War*, The Military Technical Academy Printing House, Bucharest, 2003 (in Romanian language).
- [29]Victor Greu, *Methods, Techniques and new Technologies in Communications-Vol.VI (The Multiple Access in Spread-Spectrum Communications Systems)*, The Military Technical Academy Printing House, Bucharest, 1997 (in Romanian language).
- [30]Victor Greu, Gruia Timofte, *C4I2 Integrated Communications Systems*, The Military Technical Academy Printing House, Bucharest, 2004 (in Romanian language).