

**Developing Information and Communications Technologies with More Artificial Intelligence, Using Artificial Intelligence,
When Internet of Things is “Intelligence Everywhere”
-Part 1-**

Prof. Eng. Ph.D. Victor GREU



Abstract

The paper is approaching the systemic analysis of the emergency of advanced artificial intelligence (AI) systems and generally of AI in the context of Information and Communications Technologies (ICT) exponential evolution and proliferation, as main driving factor of the transformation of the Information society (IS) toward Knowledge Based Society (KBS).

The paper analysis presents the AI premises to be a potential revolutionary step in ICT development, having, naturally, challenges of the same scale, because of the complex convergence of the state-of-the art AI technologies with Internet of Things (IoT) networks (IoT is “intelligence everywhere”!) and Big Data, applying with exponentially pace/performance at Earth scale.

Security, ethical, moral or legal rules are identified as the prominent challenges of the exponential pace/performance and planetary expansion of AI/ICT, addressed to humankind in IS toward KBS on Earth.

Among the challenges, security is first, because the benefits of the AI/ICT progress have got such a huge level and horizontal expansion in autonomous systems and processes, as our lives depend dramatically on their reliable and safe operation. Consequently, the solution is not to stop AI/ICT progress, but to use our actual intelligence and refined knowledge in order to “build robots we can trust” and generally ICT we can trust. From security point of view, developing ICT with more artificial intelligence, using artificial intelligence could create sensible risks against the essential requirements on ethical, moral or legal rules.

In detail, the analysis confirms that in the (actual or next) stage of AI/ICT development we can lose the safe limit of control for AI, when imbedded “intelligence” (as performance and technology level) is pushing us to think that we can trust in higher or total (100%) autonomy of the new AI systems only because the technology can support that (level of autonomy)!

Paper proposition is that the essence of “fight” (against advanced AI vulnerabilities) strategy has to be the plenary use of the only (long term) advantage human could have over AI (machine): the imagination potential. Consequently, when developing advanced AI/ICT (especially advanced robots), we have to use the most advanced refined knowledge plus our imagination maximum potential, aiming with priority two main objectives. First we must be sure that human subjective criteria are cleared (know yourself) by refined knowledge based on security, ethical, moral or legal rules. Then, analyse all possible scenarios of “fight” (against advanced AI vulnerabilities).

Technically we can win the “fight” (against advanced AI vulnerabilities) only if applying the advantage of using similar refined knowledge, but exceeding by human (unlimited) imagination the analysis advanced AI could perform based on learning processes it could have passed.

The analysis concludes with the crucial importance of models and algorithms the specialists could use to apply the more and more performant available technology, because this amazing AI/ICT performance and proliferation at planetary scale are the main premises to create functional vulnerabilities (risks) unless backing solutions to timely compensate them are provided by appropriate models and algorithms.

Keywords: advanced artificial intelligence, autonomous systems and processes, Internet of Things, Big Data, information society, knowledge based society, autonomous weapons.

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

1. The complex expansion of AI, IoT and Big Data in Information Society toward Knowledge Based Society

Speaking about intelligence is a very exciting issue, but not only for the modern approach of human capacity, as from ancient times we may quote Socrates [19]:

"I know that I am intelligent, because I know that I know nothing".

The chosen of Socrates modest evaluation for starting our analysis is not random, as it has a double significance.

First of all, it is a relevant opinion on main theme, but then it reveals the crucial role of refining knowledge.

More than these and our days more than ever, it amplifies and gives basics to the well known [19] Descartes thinking on methodical doubt: *"Dubito, ergo cogito, cogito, ergo sum"*.

This way we have just arrived to paper title essence, as speaking about artificial intelligence (AI) we have to carefully, although shortly, analyse what intelligence could be and ... become!

We are in the middle of such deep meditations because we have to also recognize that any progress must consider the past achievements, as Isaac Newton suggested in 1676 [19]: *"If I have seen further, it is by standing on the shoulders of giants"*.

For sure, a clear and concrete direction for analysis and action was brilliantly given by Albert Einstein [19]: *"The true sign of intelligence is not knowledge but imagination"*.

What could be more useful than imagination in our days when *Information and Communications Technologies (ICT)* pushed the *Information society (IS)* on a such high and complex evolution toward *Knowledge Based Society (KBS)*, when speed, performance and proliferation seem to have no limits, but only imagination brings our feet on ground to see Earth resources fading and our intelligence limits, for having further the chance of finding the appropriate ... intelligent solutions for the humankind future and a sustainable progress.

So we have the main pillars for approaching AI starting from what human intelligence should be today.

To be more clear, considering the emergent huge proliferation of IoT as *"intelligence everywhere"*, we have to be sure that *developing ICT with more artificial intelligence*, that *intelligence* it will be based on **the intelligence human kind should have on today's Earth**.

One could ask why we should doubt that people's intelligence is today on the right track, as this intelligence is creating ubiquitous amazing ICT products and services.

As we have already presented [9][2][5][12], the exponential pace, the progressive complexity and planetary expansion of ICT implications in all human activities and achievements have unfortunately negative consequences too.

Anyway, it is well known that the optimization of such complex and complicate processes and systems, as our World includes today, is almost impossible, taking into account, among other, just the difficulty to harmonize the optimization criteria [16]. This *does not means that the ICT development could be done exclusively by commercial criteria*.

Now it is easy to understand the necessity to approach AI, as one of the most important challenges of the ICT exponential evolution in IS on the complex road toward KBS, **a potential revolutionary step in ICT development**.

After these theoretical premises, the analysis could become more concrete and relevant by presenting some actual trends/examples of AI development in the general context of ICT.

Perhaps 20 years (or so) ago, it was simpler to give some examples of AI main domains, as expert systems, robots, war games or similar, but it is worth to mention that the *intelligence* level was also "simpler".

On the other hand it was natural to imagine that the ICT huge performances and exponential pace will push the AI also beyond incredible limits, although we have to recall that Karel Capek introduced the term robot since 1920 [3].

Our paper point is how the AI development must be managed to provide a safe and sustainable progress of AI/ICT products and services, including IoT, in the frame of IS/KBS, by timely analyzing and designing/controlling that "*incredible limits*".

In order to achieve such complicate and difficult aim it is supposed to use the appropriate human intelligence potential.

The actual dramatic challenge for this aim is the fact that today IA reached such high level to compete sometimes human intelligence [20], as surgeons work "in tandem" with surgeon-robots [1].

To completely cover the paper title background we have to mention, [3] [8], that actual AI systems could write articles (or line of codes for software), optimize integrated circuit design, auto configure ICT networks, drive autonomous cars, behave as personal assistant robots or as ... war killers robots etc.

As a matter of fact, all the above mentioned fields/examples are not the latest news, because they represent AI trends developed in the last decade (or so), now on different stages of evolution with high performance perspective.

The most prominent consequences of the actual trends come from the complex convergence of the state-of-the art AI technologies with IoT networks and Big Data algorithms and applications, applying with exponentially pace/performance at Earth scale.

This convergence is happening either in the mentioned fields or new impressing areas, as *computer vision*, a legacy of older *forms recognition* [6].

Still, perhaps a revolutionary phase/step of AI development, with resonant applications in the entire IS and further in KBS is the emergent development of ***deep learning (learning the robot to learn)***.

Without approaching in detail the above examples in the paper space, some relevant implications and challenges could reveal some AI development issues which must be carefully managed to provide a safe and sustainable progress of AI/ICT products and services, including IoT, in the frame of IS toward KBS, for humankind benefit (or even survival) on Earth.

The main challenge, associated with AI, but also generally with ICT by their huge emergent icebergs IoT, Cloud and Big Data, comes from the overwhelming influence and partially unpredictable consequences at Earth scale on long term, from vital points of view, starting with peoples/humankind security and ending with environment changes.

Focusing on AI (but easy to extend to ICT) we have to observe that the more the technologies cover all human activities and habits, along with the obvious benefits there is not only a daily dependence peoples are suffering, but slowly this tends to affect their capacity to act in some vital directions like moving, physical working, communicating, managing and eventually creating.

If these last issues could be considered minor or subjective security risks, on short term, then we have to mention some real risks that the actual AI could raise in the most complex applications.

With other words, today we are already depending on hundred of autonomous systems and processes, where planes automated pilots, surgical robots, smart home, smart grid or smart city are just a few. So, tomorrow AI could decide who is to be saved in an emergency and who is not. But after tomorrow AI could decide who to die.

In order to avoid any confusion, we have to mention that all these are features of the modern life and generally peoples cannot oppose to the technological progress observing some inherent negative implications of the process.

The point is that the benefits of that progress have got such a huge level and horizontal expansion in all mentioned autonomous systems and processes, as ***our lives depend dramatically on their reliable and safe operation***[1].

Consequently, the solution is not to stop AI/ICT progress, but to ***use our actual intelligence and refined knowledge*** in order to "***build robots we can trust***" and generally ***ICT we can trust***.

The vague term "trust" must extend our attention beyond ***reliable and safe operation***, as killer robots and generally advanced AI (intelligent robots being just a case) rise the complicate and complex problem of ***ethical, moral or legal rules to be conceived and later applied when designing, building and using AI*** [1].

Here is the point where our title could be relevant, as ***developing ICT with more artificial intelligence, using artificial intelligence*** could create sensible risks against the above essential requirement on ***ethical, moral or legal rules***.

Summarizing we can say that ***security, ethical, moral or legal rules*** are the prominent challenges of the exponential pace/performance and planetary expansion of AI/ICT, addressed to humankind in IS toward KBS on Earth.

Now the actual picture and challenges of AI development seems to be clearer, as we have estimated the main problems and we pointed the general approach for optimal solutions.

It is more than obvious that there is a long way to concrete optimal solutions, we even do not intend to approach, but we can shortly analyse some examples of actual premises, status and options for such solutions for the main AI applications domains.

The specialists agree that generally the robots represent the most important AI field, with amazing proliferation, versatility and scalability so that is why there is a huge interest for what is necessary to build robots we can trust[1]:

"To build robots that inspire trust, roboticists are working with psychologists, sociologists, linguists, anthropologists and other scientists to understand a lot more about what makes us trustworthy and reliable in all the different roles we play" (using robots!).

In fact, for every application we have to exactly define our expectations in terms of the robots capabilities, their accuracy (metrics) and the man-machine interfaces which express these parameters to the users without errors.

More than these, "our expectations" could differ (at planetary scale), especially when we have to define ***security, ethical, moral or legal rules limits for robots***.

Again we have to observe that we see only the iceberg tip[5][16], as to define the above metrics and limits is a complex multidisciplinary optimization process and specialists recognize that today "We don't know to do that well yet" [1].

In addition we consider that the problems, although similar when passing from robots to a huge diversity of applications involving AI, could be even more complicated sometimes by the fact that the probable trend is to give to AI systems more and more autonomy (for example in autonomous cars, military robots etc.) as performance and technology limits are higher and higher[8].

Finally we have just arrived to ***the dilemma suggested by the paper title: in the (actual or next) stage of AI/ICT development we can lose the safe limit of control for AI, when imbedded "intelligence" (as performance and technology level) is pushing us to think that we can trust in higher or total (100%) autonomy of the new (designed) AI systems, only because the technology can support that (level of autonomy)***!

It could be surprising, but this dilemma is not new, as least we presented it [20] in a general form for ICT, but anyway the essence is that we have arrived at that performance and technology where ***the competition man-machine could be won by the machine in more and more domains of AI***.

Here we have to recall that it started with "computing", then chess followed, but today we speak about another stage, when surgeon is working in tandem with the robot and the commander could be replaced in a complex/dynamic/special decision system by the killer robot.

The question is Why/How these situations could exceed the safe limit?

A first (simple) answer is because the safe limit will be more and more difficult to define, measure and eventually control, just because we are faster introducing AI in systems more and more complex and difficult to mathematically model by deterministic algorithms (but by heuristics or statistical ones).

A second (more elaborated) answer has to consider the first and then add the fact that human could not compete the advanced AI systems because, along with the computing power, the system usually includes complex networks of sensors (here comes IoT!) which provide an enormous amount of data transformed in knowledge (here comes Big Data!) and when the moment of (fast or dynamic) decision comes, **human really has no chance (numerical arguments or data) to counter the AI system, because all the available information is that provided by the AI system.**

Is then really nothing we can do?

No, we still have options, till it is not too late!

Then what to do?

Remember Newton (the above quote) to "see further" and then remember Einstein (the above quote) to use imagination and then fight ... knowledge!

Because it is not a simple fight it is better to analyse it (of course not exhaustively) in the next section.

2. Building robots without being robots

As we can find Newton's "giants" either after or before him, here it is worth to quote the ancient Sun Tzu: ***"know yourself and you will win all battles"***.

We have considered starting the "fight" (against advanced AI vulnerabilities) with Sun Tzu advice because the roots of AI intelligence (or lack of it!) must be searched in ... our intelligence (or lack of it!).

The essence of "fight" strategy is to plenary use, as we already suggested[9][12][20], *the only (long term) advantage human could have over AI (machine): **the imagination potential.***

Consequently, when developing advanced AI/ICT (especially, advanced robots), we have to use the most refined knowledge plus our imagination maximum potential, aiming with priority two main objectives.

First we must *be sure that human subjective criteria are cleared (know yourself) by refined knowledge based on **security, ethical, moral or legal rules.***

Then, remembering Socrates (the above quote) and Descartes (the above quote), ***analyse all possible scenarios of "fight" (against advanced AI vulnerabilities).***

Before any other concrete step, we consider again appropriate to recall a Sun Tzu quote, ***"opportunities multiply as they are seized"***, because we have to use timely the acquired technological progress, anticipating all its positive or negative consequences.

Now a concrete step is to deeply understand, everyday and every way we think or act, Descartes' message on methodical doubt (the above quote, in section 1).

Especially when we analyse and design advanced AI/ICT (i.e. advanced robots), methodical doubt is crucial in combination with the state-of-the-art refined knowledge valued by human superior imagination, in order to extend the multicriteria analyses to all possible (and even impossible) scenarios.

Technically and simpler speaking, we can win the “*fight*” (*against advanced AI vulnerabilities*) only if applying the advantage of using similar refined knowledge, but exceeding by human (unlimited) imagination the analysis advanced AI could perform based on learning processes it could have passed mainly by neural networks models and algorithms.

To be more specific, usually AI systems perform their advanced processes by neural networks models and algorithms which are applied to diverse sets of collected (or learned) data through designed sets of rules.

On the other hand, the specialists intelligence could use the human (unlimited) imagination to exceed the AI by the fact that they have conceived the sets of rules and had **the chance to anticipate the AI operation rules (technology) limits**.

Notice that it is essential to understand the crucial importance of models and algorithms the specialists could use to apply the more and more performant available technology[16], because, as we above mentioned, this amazing AI/ICT performance and proliferation at planetary scale are the main premises to create functional vulnerabilities (risks) unless backing solutions to timely compensate them are provided by appropriate models and algorithms.

All the above premises represent a valuable motivation for better understanding why and how **building robots without being robots** is a prominent requirement, as AI/ICT designers have to be a step ahead against advanced AI vulnerabilities, using the above mentioned **chance to anticipate the AI operation rules (technology) limits**.

More than these, we consider that when developing ICT with advanced AI, using artificial intelligence, especially in the (future) cases where machines will have a substantial role in design processes, involved human must avoid the routine approach (*not being “robot” in the dynamic world of AI/ICT!*), providing instead the appropriate control for safety, in the design phase by models, algorithms and in the operation phase by user hard/soft redundant interfaces.

If someone could think that these redundant analyses, risk evaluations and hard/soft safety measures are overdone, it is relevant to remember a quote[19] of another “giant”, Stephen Hawking, about intelligence and life safety:

“I believe alien life is quite common in the universe, although intelligent life is less so. Some say it has yet to appear on planet Earth”.

Also as a confirmation of our above approach about control and timely react, Stephen Hawking said: *“Intelligence is the ability to adapt to change”.*

Of course, all these general directions are essential, but always we have to remember that real life is much more complicated. Perhaps that is why Stephen Hawking did more than giving good advices.

In fact, the importance and realism of the subject of our paper are also confirmed by a group of leading researchers in AI [3], which called in 2015 for a ban on “*offensive autonomous weapons beyond meaningful human control*”.

More than this, at an AI conference, the group presented an open letter where they warned about a “*global AI arms race*”.

The impact of this letter[3] is expressed by the fact of being “*signed by more than 20,000 people, including such luminaries as physicist Stephen Hawking and Tesla CEO Elon Musk, who last year donated US \$10 million to a Boston-based institute whose mission is “safeguarding life” against the hypothesized emergence of malevolent AIs*”.

It is sure that AI/ICT challenges go beyond *malevolent AIs*, as we have presented above, but is also truth that autonomous weapons are one of the biggest AIs dangers for humankind future.

Methodical doubt taught us to use our imagination, for example to answer to a logical question: *could be some other AI more dangerous than autonomous weapons?*

Of course it is very difficult, in spite of all the above paper considerations, to answer this question or simply say: Yes.

Just recall from the title that **IoT is “intelligence everywhere”** and we can imagine from here the huge diversity of emergent applications where IoT, Cloud, Green ITC and Big Data will be extended at planetary scale [15][5][7][11][10][13][14][17][18].

Again some examples could be relevant by AI potential impact on humankind life:

- ICT future advanced networks (mainly Internet, but not exclusively);
- Smart grid for power networks optimization;
- Industrial robots and AI systems (just imagine nuclear, chemical, petroleum, gas etc.);
- Autonomous transportation (planes/cars/trains pilots etc.)
- Environment monitoring/protection systems;
- Security systems.

After shortly analysing every example, it is easy to imagine a scenario where unreliable operation of AI systems could have dramatic consequences over a huge number of people or communities, even exceeding what a killing robot could do, but we have to also mention that autonomous weapons could include rockets and so on.

In this relative comparison, but also in the above analyses, we did not mention perhaps the most dangerous risk for humanity today: the terrorism.

If in the past decades the defence/security authorities spoke about what if a dirt nuclear bomb would be in the hands of terrorists, in our days they speak more and more about cyber-attacks or cyber-space security.

It is not difficult to imagine that sooner or later the AI will be involved in the most sophisticated security systems.

If today AI is involved in writing code lines (lets say, for simple/partial applications) or in computer vision systems, it is clear that here the future will bring more and more essential involvement and ... potential vulnerabilities, including criminal actions.

The last observation is obviously more that it could appear, because the scenario is possible not only in a security system, but ... everywhere (including all above examples!).

Coming back to the above start (**IoT is “intelligence everywhere”**), we can only to observe that all examples (and more) could be in a way or other, less or more, sooner or later, under IoT “umbrella” – or under Internet or any other future net!

That is why we have to agree that the paper subject needs to be continued.

3. Conclusions

The paper analysis showed that AI represents a potential revolutionary step in ICT development, having, naturally, challenges of the same scale, because of the complex convergence of the state-of-the art AI technologies with IoT networks and Big Data, applying with exponentially pace/performance at Earth scale.

Security, ethical, moral or legal rules are the prominent challenges of the exponential pace/performance and planetary expansion of AI/ICT, addressed to humankind in IS toward KBS on Earth.

The benefits of the AI/ICT progress have got such a huge level and horizontal expansion in autonomous systems and processes, as **our lives depend dramatically on their reliable and safe operation.**

Consequently, the solution is not to stop AI/ICT progress, but to **use our actual intelligence and refined knowledge** in order to “**build robots we can trust**” and generally **ICT we can trust.**

Developing ICT with more artificial intelligence, using artificial intelligence could create sensible risks against the above essential requirement on *ethical, moral or legal rules*.

In the (actual or next) stage of AI/ICT development we can lose the safe limit of control for AI, when imbedded "intelligence" (as performance and technology level) is pushing us to think that we can trust in higher or total (100%) autonomy of the new AI systems **only because the technology can support that (level of autonomy)!**

The essence of "fight" strategy is to plenary use, as we already suggested[9][12][20], *the only (long term) advantage human could have over AI (machine): the imagination potential*.

Consequently, when developing advanced AI/ICT (especially, advanced robots), we have to use the most refined knowledge plus our imagination maximum potential, aiming with priority two main objectives.

First we must *be sure that human subjective criteria are cleared (know yourself) by refined knowledge based on security, ethical, moral or legal rules*.

Then, remembering Socrates (the above quote) and Descartes (the above quote), ***analyse all possible scenarios of "fight" (against advanced AI vulnerabilities)***.

The essence of "fight" strategy is to plenary use, as we already suggested[9][12][20], *the only (long term) advantage human could have over AI (machine): the imagination potential*.

Consequently, when developing advanced AI/ICT (especially, advanced robots), we have to use the most refined knowledge plus our imagination maximum potential, aiming with priority two main objectives.

First we must *be sure that human subjective criteria are cleared (know yourself) by refined knowledge based on security, ethical, moral or legal rules*.

Then, remembering Socrates (the above quote) and Descartes (the above quote), ***analyse all scenarios of possible "fight" (against advanced AI vulnerabilities)***.

Technically we can win the ***"fight" (against advanced AI vulnerabilities)*** only if applying the advantage of using similar refined knowledge, but exceeding by human (unlimited) imagination the analysis advanced AI could perform based on learning processes it could have passed.

The analysis reveals the crucial importance of models and algorithms the specialists could use to apply the more and more performant available technology, because this amazing AI/ICT performance and proliferation at planetary scale are the main premises to create functional vulnerabilities (risks) unless backing solutions to timely compensate them are provided by appropriate models and algorithms.

REFERENCES

- [1] Susan Hassler, *Building robots we can trust*, IEEE Spectrum, June 2016.
- [2] Victor Greu, *The information society towards the knowledge based society driven by the information and communications technologies - from the Internet of Things to the Internet of ...trees (Part 1)*, Romanian Distribution Committee Magazine, Volume 6, Issue1, Year 2015.
- [3] Erico Guizo, Evan Ackerman, *When robots decide to kill*, IEEE Spectrum, Jun 2016.
- [4] *** *More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020*, ABI Research, London, United Kingdom - 09 May 2013, www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne/

- [5]Victor Greu, *Information and communications technologies go greener beyond IoT- behind is all the Earth-(Part 1)*, Romanian Distribution Committee Magazine, Volume 7, Issue2, Year 2016.
- [6]Prachi Patel, *Fatih Poriklisets the bar for computer vision*, , IEEE The Institute, Jun 2016.
- [7]*** *Internet of Things — An action plan for Europe*, (PDF). COM(2009)-278 final, Commission of the European Communities -18 June 2009.
- [8]Nathan A. Greenblatt, *Self driving cars and the law*, IEEE Spectrum, Feb 2016.
- [9]Victor Greu, *Searching the right tracks of new technologies in the earth race for a balance between progress and survival*, Romanian Distribution Committee Magazine, Volume 3, Issue1, Year 2012.
- [10]Ke Xu et all, *Toward software defined smart home*, IEEE Communications, May 2016.
- [11]Kathy Pretz, *A toolkit for building energy-efficient communications networks*, IEEE The Institute, May 2016.
- [12]Victor Greu, *The Exponential Development of the Information and Communications Technologies – A Complex Process Which is Generating Progress Knowledge from People to People*, Romanian Distribution Committee Magazine, Volume 4, Issue2, Year 2013.
- [13] Mark Harris, *The Internet of Trees*, IEEE Spectrum, Mar.2014.
- [14] Rebecka Jarbur, *Developing guidelines for green information and communication technology* - (Thesis at) Dept. of computer and information sciences university of Strathclyde, September 2014.
- [15]Agarwal, S. and Nath, A., *A study on implementing Green IT in Enterprise 2.0*, International Journal of Advanced Computer Research, 2013, pp. 43-49.
- [16]Victor Greu, *Context-aware communications and IT – a new paradigm for the optimization of the information society towards the knowledge based society (Part 2)*, Romanian Distribution Committee Magazine, Volume 5, Issue4, Year 2014.
- [17]Prechi Patel, *Building a more eco-friendly telecom industry*, IEEE The Institute, Mar.2016.
- [18]Kathy Pretz, *Environmentally friendly Information and Communications Technologies*, IEEE The Institute, Mar.2016.
- [19]***, https://www.brainyquote.com/quotes/topics/topic_intelligence.html
- [20]Victor Greu, *Tomorrow's paradox: refining knowledge by smarter information and communications technologies while humans tend to become a limited factor of performance*, Romanian Distribution Committee Magazine, Volume 7, Issue1, Year 2016.