

Information and Communication Technology is Supporting People to Refine Knowledge Because a Safe Balance of Artificial and Human Intelligence Could Leverage the Search for the Right Tracks of World Evolution

-Part 3-



Prof. Eng. Ph.D. Victor GREU

Abstract

The paper analysis is approaching factors implied in KR processes, aiming the sustainable progress we need when facing the actual World dramatic crises and challenges, as climate changes, global warming, Earth resources fading, social unbalances, geopolitical conflicts etc., considering that the material consequences could ask first for “business continuity”, keeping as much as possible the previous level if not a substantial progress, where the economy/industry growth, including ICT, could be a relevant example. Knowing the ICT exponential development, this is linked with Moore’s Law, as it resulted when analysing, as example, the radical innovations of video processing technology made by Nvidia, which generated a wave of technological progress among competitors, as a new standard, witnessing that Moore’s Law is not dead. We have to notice, among many technical details, that ICT has the same potential to re-invent itself, even in hard conditions, which is the essential belief for considering the prominent role of ICT for IS/KBS, we repeatedly mentioned as one of the strongest resources on Earth, for innovation and general progress. Along with obvious and unprecedented benefits, ICT/AI could bring vulnerabilities and risks (we also did not encounter and even would not imagine, especially considering the World dramatic crises, threats and challenges), mainly by the high speed of technology which reduces the time of refining the knowledge and adapting to changes, for both organization and individual levels. In the same time, ICT advances, recently including AI, is providing potential fast instruments for law crossing actions, now mainly inside the cyber-crime areas, but not exclusively, as social media networks are another obvious case. Here we can see cyber-crime outlaws only as “iceberg tips”, a metaphor for revealing the emergence of other huge challenges and threats, even beyond ICT direct influence, as hybrid wars, war crimes and many other cases of law or rules disregard, which recently tend to show a trend to a less rules World, where more people, organizations and even states prefer to ignore the traditional principles and values based on rules and laws, nearly promoting the law of force/power as a new approach of human relations and generating a natural worry for the future of Earth and humankind, because all these grow as roots of some World crises, affecting, among others, the economic relations/circuits on which any sustainable progress would be based, but also the humans peaceful lives. At planetary scale, these crises and threats, first mentioning the consequences of geopolitical/military conflicts, hybrid wars, cyberattacks etc., rise a series of negative trends for states and people, as spiral of military spendings, spiral of destruction, spiral of economic losses, spiral of hate, spiral of dehumanization, spiral of fear etc., which add to the already dangerous evolutions/context of Earth ecosystem we have mentioned. This way, it resulted, by examples starting in 2024 and dealing with unprecedented cyberattacks, that these “iceberg tips” could indicate ways to imagine and approach a part of the complex issues of KR, identifying some potential causes of World crises and threats. **These reveal in fact the essential role/potential of exponential development of ICT to create benefits and vulnerabilities for the entire World, but also to defend Earth ecosystem. It is clear that extracting and refining knowledge from these dynamic and unpredictable realities, in order to provide a sustainable progress in all areas where ICT proliferates, represent a long and complicated road which needs timely and deeper analyses.**

*In the second section we have analysed some strange evolutions on the actual challenging ICT/World context, where liberty and democracy tend to be confused with disregarding or even rejecting the rule of law, logic and generally of science, without speaking of disrespect for humankind traditional values and principles, as ethics and moral ones, so often present in social media networks, where fake news, manipulation or violence are going up to hybrid war forms. **When it appears an impossibility to solve very difficult problems or further rule the turbulent World, some people believe that instead of a scientific approach they could use an intuitive/heuristic one, or instead of correct/moral behaviour they could come back to the jungle rule of force, all these because other solutions are not foreseen and unfortunately not properly searched.***

Detailing the analysis of cyber-crime domain, we could observe how deep and knowledge revealing this could be, from some examples, starting with the Blue Pill shocking reference on the 1999 movie The Matrix. Step by step we see that, with IoT, starting from home, we suddenly could be in fact at the strategical level of critical and national infrastructures. As if there were not enough scaring scenarios, at once we jump in the highest conflicts of the World, as it is also confirmed by recent examples. We also have noticed the AI potential to request multi-criteria analyses in order to optimize the sustainable progress it would provide for the emerging challenging World, using collected data and showing how accurately and ethically data should be handled, because it directly impacts system performance and user acceptance.

Concluding, but going even beyond ethics, rules and laws, using all new data, information and knowledge from the entire Earth ecosystem, in order to learn and benefit, all these could impact individuals, companies, organizations and states, as, consequently, we consider that, in the actual and emerging World challenges and crises context, the role of KR is essential and mandatory to be found and implemented, as one of the most efficacious and efficient leverage to sustainable progress, everywhere humans live, scaling and spreading from individual thinking, behaviour and actions, but also reaching the incumbents and leaders of large entities.

Keywords: Moore's Law, graphics processing unit (GPU), distributed denial of service (DDoS), cyberattack (Blue Pill, The Matrix), knowledge refining (KR), artificial intelligence, IoT, AI/Data Ethics

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

***“Where is the wisdom we have lost in knowledge?
Where is the knowledge we have lost in information?”
— T.S. Eliot***

1. ICT is alive: from keeping up Moore's Law to supporting a less rules World

Our previous articles stressed on how to refine knowledge, as the World, along with the information and communication technology (ICT), are very fast changing, but the right ways to do that are by far the most important question for everyone is trying to improve it. That is why we will continue to analyse the context, the premises and the opportunities where ICT, including artificial intelligence (AI), could contribute on supporting humans, besides human intelligence (HI), to find the best ways toward knowledge refining (KR), which helps to provide, for people and the Earth ecosystem, the sustainable progress we need when facing the actual World dramatic crises and challenges, as climate changes, global warming, Earth resources fading, social unbalances, geopolitical conflicts etc. [3].

Although, in extreme and unpredictable conditions, sometimes it is better to look for refined paradigm changes, the actual World material crises/challenges (see, for example, Earth resources fading, geopolitical conflicts or war destructions) could ask first for having the known security approach for “business continuity”, as a metaphor for keeping as much as possible the previous level if not a substantial progress, where the economy/industry growth could be a relevant example[8][10][12][14][16][19][18][21].

Especially for the ICT exponential development, the above approach is linked with Moore's Law, among other essential factors of progress, as it is also detailed in [1]:

“Nvidia was the first company to offer a fully integrated graphics processor for PCs, in August 1999, which they named GPU, and the acronym has been with us since. The primary differentiating element of Nvidia’s pioneering GeForce 256 was its hardware transform and lighting (T&L) engine, which offloaded geometry calculations from the CPU. The T&L engine then fed four fixed pixel pipelines, each capable of applying a single texture at a time. Nvidia introduced its first GPU with programmable shaders with the GeForce 3 series (NV20) in February 2001, a significant advancement over the GeForce 256’s fixed-function pipelines. And so, the shader era began in 2001. The GeForce 3 featured four pixel shaders and a vertex shader. Since then, 18 years later, the programmable shader architecture has expanded, gotten more plentiful, faster, and relatively smaller. The GeForce 3 was built using a 150 nm process. That allowed Nvidia to pack 57 million transistors onto the NV20 die, which had a die area of 128 mm². Today’s Blackwell (B100) design has 92 billion transistors, incorporating 24,064 shaders in a 750 mm² die.”

Here we could observe not only impressing evolutions of keeping Moore’s Law (the number of transistors on a microchip doubles roughly every two years), but also radical innovations of video processing technology made by Nvidia:

“After the GPU was introduced, Nvidia started branching out into different PC segments such as workstation, mobile, and computational. But the gaming market had always been the big one for from 2002 to 2005 graphics AIB’s GPUs were primarily differentiated by clock frequency. With the introduction of the GeForce 7 Series and GeForce 8 Series, Nvidia began distinguishing between entry-level, mid-range, and high-end gaming GPUs by shader count. Between August 2005 and July 2007 Nvidia introduced 26 versions of the GeForce 7 series with pixel shader counts ranging from 2 to 24, and a variety of vertex shaders. It was pretty chaotic as Nvidia tried to fill every market segment niche.”

It is also worth noting that Nvidia not only impressively progressed, but in same time generated a wave of technological progress among competitors, as a new standard:

“Then, and thereafter, Nvidia (and its competitors) differentiated GPUs by shader count for the main gaming segments, which at that time were Value (or Entry), Low-end (or Mainstream), Midrange (or High-end), and High-end (AKA Enthusiast). The Value segment would get wiped out by ever more powerful iGPUs in the CPU between 2011 and 2015. Ironically, AMD which made some of the first iGPUs (they called APUs) was the last company to abandon the Value segment. From 2007 to 2025, the shader count went from 16 (low end) to 128 (Enthusiast high-end), to 3,840 (Entry-level) to 21,760 (High-end), a 2,3900% to 16,900% respectable. Or stated another way, 1,406% to 994% per year. That rate is of course much faster than Moore’s law and one of the reasons GPU vendors said (and still do) that they are increasing performance faster than Moore’s law (which by the way, is not dead).”

This way we could witness that Moore’s Law is not dead, but, further, on the other side, perceive the physical difficulties to keep it up, while the economic success is also a big challenge for the base of what we may consider, perhaps, one of the most dynamic industry on Earth:

“Nvidia introduced Tensor Cores as part of their Volta GPU architecture during 2017. This early version of the technology was incorporated into the Tesla V100, a GPU developed with machine learning and artificial intelligence applications in mind. Following this, Tensor Cores became a common component within Nvidia’s GeForce RTX line of graphics processing units intended for gaming. Their inclusion began with the initial RTX cards, which were built upon the Turing architecture and released in 2018, and thus began the era of AI GPUs. AI will use every shader available to it and ask for more... With all the technological development in hardware, the price of the GPU add-in boards (AIBs), hasn’t risen nearly as fast of as much. In 2007 a high-end enthusiast, AIB, sold for \$600 to \$800. In 2025 the high-end RTX 5090 sold for \$1,900, just 150% more in 18 years. The inflation rate from 2007 to today is 159%, so an

\$800 2007 AIB would cost \$1,270 today, adjusted for inflation, the cost of an AIB with 994% more shaders would only cost 57% more.”

This short evolution convincingly revealed the exponential evolution of ICT, but, on the other hand, we see some actual, nearly unpredictable, trends like the rise of new industry leaders (as Nvidia), in spite of the obvious difficulties to grow on recent difficult times.

Still, we observe, among many technical details, that ICT has the same potential to reinvent itself, even in hard conditions, which is the essential belief for considering the prominent role of ICT for Information Society (IS) toward Knowledge Based Society (KBS), we repeatedly mentioned, [11][22], as one of the strongest resources on Earth, for innovation and general progress.

On the other hand, as we also long time ago presented [9], the last stages of ICT and IS/KBS, along with obvious and unprecedented benefits for the Earth ecosystem and human life/evolution, could bring vulnerabilities and risks we also did not encounter and even would not imagined, especially considering the context of all emergent World dramatic crises, threats and challenges above mentioned.

Consequently, we have to observe that the influence of ICT on such global challenges is important mainly by the high speed of technology which reduces the time of refining the knowledge and adapting to changes, for both organization and individual levels.

In the same time, ICT advances, recently including AI, is providing potential fast instruments for law crossing actions, now mainly inside the cyber-crime areas, but not exclusively, as social media networks are another obvious case.

At this point, we can see cyber-crime outlaws only as “iceberg tips”, a metaphor for revealing the emergence of other huge challenges and threats, even beyond ICT direct influence, as hybrid wars, war crimes and many other cases of law or rules disregard, which recently tend to show a trend to a less rules World, where more people, organizations and even states prefer to ignore the traditional principles and values based on rules and laws, nearly promoting the law of force/power as a new approach of human relations and generating a natural worry for the future of Earth and humankind, because all these grow as roots of some World crises, affecting, among others, the economic relations/circuits on which any sustainable progress would be based, but also the humans peaceful lives.

We have to point that, at planetary scale, these crises and threats, first mentioning the consequences of geopolitical/military conflicts, hybrid wars, cyberattacks etc., rise a series of negative trends for states and people, as spiral of military spendings, spiral of destruction, spiral of economic losses, spiral of hate, spiral of dehumanization, spiral of fear etc., which add to the already dangerous evolutions/context of Earth ecosystem we have mentioned above (climate changes, global warming, Earth resources fading, social unbalances) and earlier [9][20].

Now it is obvious that analysing such negative trends and the ways to mitigate them is a straight direction to identify and update the prominent, complex and dynamic factors to be continuously approached by KR.

In this context, we consider that the next examples (starting in 2024), dealing with unprecedented cyberattacks, as “iceberg tips” they could indicate ways to imagine and approach a part of the complex issues of KR, identifying some potential causes of World crises and threats which are linked with ICT[2]:

“The most powerful distributed denial of service (DDoS) attack ever was launched in September, but caused little to no damage. That’s according to Cloudflare, a web security provider, which said its systems automatically detected the attacks, absorbing the massive influx of traffic across its own servers before it could flood and take down websites and apps like a DDoS normally would. The attacks peaked when the unknown hackers sent traffic at 3.8 terabytes per second to a target server, mostly firing data sent over the User Datagram

Protocol (UDP), peaking at 2.14 billion packets per second. UDP is typically used for apps that need fast data transfer, like online video chat and games. The attack came as part of a month-long campaign, which combined the power of hacked networking equipment and web servers. The attackers were targeting customers across different industries from finance to telecoms, Cloudflare wrote in its report on the attacks.”

We have to notice the danger of relativity of evaluation of such events and trends, as depending on targets/victims assets and reliability:

<<“What’s astonishing is the attacker’s ability to orchestrate these various devices to launch coordinated attacks,” CloudFlare said. “The scale and frequency of these attacks are unprecedented,” Cloudflare said. “Due to their sheer size and bits/packets per second rates, these attacks have the ability to take down unprotected internet properties, as well as internet properties that are protected by on-premise equipment or by cloud providers that just don’t have sufficient network capacity or global coverage to be able to handle these volumes alongside legitimate traffic without impacting performance.”>>

These “iceberg tips” rise in fact the essential role/potential of exponential development of ICT to create benefits and vulnerabilities for the entire World, but also to defend Earth ecosystem. In the same time, it is clear that extracting and refining knowledge from these dynamic and unpredictable realities, in order to provide a sustainable progress in all areas where ICT proliferates, represent a long and complicated road which needs timely and deeper analyses.

2. Refining knowledge by understanding the ICT links from vulnerabilities to security/defence

Although the use of metaphors could appear not very inspired in these analyses, we want to emphasize just some strange evolutions on the actual challenging ICT/World context, where liberty and democracy tend to be confused with disregarding or even rejecting the rule of law, logic and generally of science, without speaking of disrespect for humankind traditional values and principles, as ethics and moral ones, so often present in social media networks, where fake news, manipulation or violence are going up to hybrid war forms.

With other words, in the complex and complicate Earth ecosystem context, where humankind is evolving between apogee and survival [9], when it appears an impossibility to solve very difficult problems or to further rule the turbulent World, some people believe that instead of a scientific approach they could use an intuitive/heuristic one, or instead of correct/moral behaviour they could come back to the jungle rule of force, all these because other solutions are not foreseen and unfortunately not properly searched.

On such premises, here we consider that the role of KR is essential and mandatory to be found and implemented, all over the World, scaling from individual thinking, behaviour and actions, but also reaching the incumbents and leaders.

Further, continuing the above analysis of cyber-crime domain, we could observe how deep and knowledge revealing this could be, from the next examples, starting with the shocking reference from the 1999 movie *The Matrix*: [4]:

<<In a world where interconnected devices dominate our personal and professional lives, the recent “Blue Pill” attack reminded us of the vulnerabilities inherent in the Internet of Things (IoT). The Blue Pill is a reference from the 1999 movie The Matrix. The “red pill versus blue pill” choice was to take a pill to either reveal the truth (red pill) or be unaware of being controlled (blue pill). This Blue Pill is now considered an advanced cyberattack. This idea was developed by cybersecurity expert Joanna Rutkowska, where a malicious virtual machine gains control of the victim’s machine. Affecting more than 35 million routers globally, this attack exploited flaws in consumer-grade devices, allowing attackers to hijack networks and

potentially launch more significant, more devastating assaults. This attack can cause network degradation for home users as well as disruption from operations, cybercrime, and reputation damage. >>

From this story of *Blue Pill*, beyond observing a similar historical resonance of terms with Bluetooth communications technology, this way we could understand the complexity of cyber-crime approaches, i.e., even the research and monitoring of this domain represent a strange mix of security real events analysis, as above presented in [2], and security virtual/vulnerability events analysis [4], further detailed and applied on the huge and emergent domain of Internet of Things (IoT):

“IoT devices form the backbone of modern infrastructure, connecting everything from home networks to critical national systems. The Blue Pill attack highlights the urgent need for a comprehensive approach to IoT security to protect not just individual users but also the stability of national infrastructure...The proliferation of IoT devices in homes has revolutionized convenience. Smart thermostats adjust temperatures based on our preferences, connected security cameras provide peace of mind, and voice assistants simplify daily tasks. However, these conveniences often come with significant security tradeoffs. Many consumer IoT devices are shipped with default passwords, rarely receive firmware updates, and are designed with minimal security considerations. These vulnerabilities make them easy targets for attackers. Worse, compromised devices can act as gateways, granting attackers access to more extensive networks, including corporate systems, when employees work remotely. The threat extends beyond individual households, underscoring the importance of securing even the most mundane devices.”

As we also presented [23][13][6], step by step we see that starting from home, we suddenly could be in fact at the strategical level of critical and *national infrastructures*:

“The Fourth Industrial Revolution brought digital transformation to industries not only through automation but data exchange. The industrial sector’s reliance on IoT devices has revolutionized operations and introduced new vulnerabilities. Industrial IoT (IIoT) devices are integral to energy grids, transportation networks, and health-care systems. Smart sensors monitor power distribution, traffic management systems optimize flow, and connected medical devices enable better patient care and management of chronic conditions. However, their critical nature makes them prime targets for attackers. The 2021 Colonial Pipeline ransomware attack highlighted the importance of cybersecurity, critical infrastructure vulnerabilities, and the growing threats. This attack was a stark example of what’s at stake, as it disrupted fuel supplies across the eastern United States, causing widespread panic and economic damage. Such incidents reveal the fragility of critical systems when IIoT devices are compromised. The risks extend beyond operational downtime to encompass public safety and national security.”

More than these, as if there were not enough scaring scenarios, at once we jump in the highest conflicts of the World, as it is also confirmed by [5]:

<<With almost 35 million devices being identified as vulnerable worldwide, threat intelligence researchers from Aqua Nautilus have warned that the Matrix could be slowing down internet speeds for home users of affected routers and exposing businesses to operational disruption, cybercrime and reputational damage. The distributed denial-of-service campaign was masterminded by a threat actor called Matrix, Morag said, and “demonstrates a growing trend among threat actors to target vulnerabilities and misconfigurations across internet-connected devices, particularly IoT and enterprise systems.” In the case of Matrix, the DDoS campaign has combined a whole bunch of things to create a formidable botnet: public scripts, brute-force attacks as well as weak credentials exploitation. The Aqua Security report suggests that the Matrix threat actor is likely Russian, but with no direct targeting of Ukrainian victims, it would appear the motivation is purely financial rather than political in this instance. What the threat intelligence does highlight, however, is the continuing evolution of the DDoS threat

within an ever-changing landscape “where even script kiddies can leverage open-source tools to execute sophisticated and large-scale campaigns,” Morag said. >>

Just because the chances of easy proliferation of such threats are fast increasing, we believe that a realistic approach of complex processes of KR, even if using the powerful instruments and findings of ICT advances, including more and more AI, should consider, among other criteria of sustainable progress, the appropriate ethical standards.

Here we have to recall that, in spite of the huge interest and applications fields linked with AI, the ethical standards and also the security issues are among the most difficult to improve areas of AI development, while the lack of such features has a major impact not only by the conformity point of view, but mainly on economy, by trust and reputation, as it is also approached by [7]:

<<In an era where data is often described as the “new oil,” its management transcends basic operational considerations and becomes integral to organizational trust and sustainability. Ethical data practices, including transparency and informed consent, have emerged as compliance requirements and strategic differentiators for business growth and customer retention...Ethical data use is essential for building customer trust, which drives brand loyalty and helps companies establish lasting market dominance. Organizations that disclose their data usage practices while implementing straightforward consent systems develop stronger customer bonds. Multiple digital transformation projects demonstrate that organizations that enforce data policies transparently achieve better customer retention. >>

Speaking of AI, we have to recall that we repeatedly [15] [17] [22] [6] presented its potential to request multi-criteria analyses in order to optimize the sustainable progress AI would provide for the emerging challenging World, using collected data, as it is further confirmed, showing *how accurately and ethically data is handled because it directly impacts system performance and user acceptance:*

*“Three emerging technologies, which combine AI-assisted data classification with real-time consent management and decentralized identity protocols, will define the future of ethical data handling: **Consent management.** Organizations benefit by conducting consent management dashboard tests alongside auditability integration and AI tool evaluations to detect potential ethical risks before they occur. **Zero-trust frameworks.** Implementing zero-trust frameworks with dedicated ethics review boards represents a strategic approach to handling changing data ethics environments. The governance models allow organizations to make agile and responsive ethical decisions throughout their structures. **Standardize data ethics.** It is vital for organizations to standardize their data ethics procedures for global operations to exceed basic regulatory standards like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Universally applying standards that exceed minimum legal requirements facilitates global operations, decreases compliance risks, and strengthens brand trust and consumer confidence.”*

Concluding, but going even beyond ethics, rules and laws, using all new data, information and knowledge from the entire Earth ecosystem, in order to learn and benefit, all these could impact individuals, companies, organizations and states, as consequently we consider that, in the actual and emerging World challenges and crises context, the role of KR is essential and mandatory to be found and implemented, as one of the most efficacious and efficient leverage to sustainable progress, everywhere humans live, scaling and spreading from individual thinking, behaviour and actions, but also reaching the incumbents and leaders of large entities.

3. Conclusions

How to refine knowledge, as the World, along with ICT, are very fast changing, is a perpetual issue, because the right ways to do that are by far the most important question for everyone is trying to improve it, recalling that knowledge refining (KR) could help to provide, for people and the Earth ecosystem, the sustainable progress we need when facing the actual World dramatic crises and challenges, like climate changes, global warming, Earth resources fading, social unbalances, geopolitical conflicts etc. [3]. The actual World material crises/challenges (see, for example, Earth resources fading, geopolitical conflicts or war destructions) could ask first for having the known security approach for “business continuity”, as a metaphor for keeping as much as possible the previous level if not a substantial progress, where the economy/industry growth could be a relevant example [8] [10] [12] [14] [16] [19] [18] [21]. Considering ICT exponential development, this approach is linked with Moore’s Law, among other essential factors of progress, as it resulted when analysing an example from [1], along with radical innovations of video processing technology made by Nvidia, which generated a wave of technological progress among competitors, as a new standard, witnessing that Moore’s law is not dead, but, further, on the other side, showing the physical difficulties to keep it up, while the economic success is also a big challenge for the base of what we may consider, perhaps, one of the most dynamic industry on Earth.

We have to notice, among many technical details, that ICT has the same potential to re-invent itself, even in hard conditions, which is the essential belief for considering the prominent role of ICT for IS/KBS, we repeatedly mentioned [11][22], as one of the strongest resources on Earth, for innovation and general progress.

As we also long time ago presented [9], the last stages of ICT and IS/KBS, along with obvious and unprecedented benefits for the Earth ecosystem and human life/evolution, could bring vulnerabilities and risks we also did not encounter and even would not imagined, especially considering the context of all emergent World dramatic crises, threats and challenges above mentioned. Here, the influence of ICT on such global challenges is important mainly by the high speed of technology which reduces the time of refining the knowledge and adapting to changes, for both organization and individual levels. In the same time, ICT advances, recently including AI, is providing potential fast instruments for law crossing actions, now mainly inside the cyber-crime areas, but not exclusively, as social media networks are another obvious case. In a way, we can see cyber-crime outlaws only as “iceberg tips”, a metaphor for revealing the emergence of other huge challenges and threats, even beyond ICT direct influence, as hybrid wars, war crimes and many other cases of law or rules disregard, which recently tend to show a trend to a less rules World, where more people, organizations and even states prefer to ignore the traditional principles and values based on rules and laws, nearly promoting the law of force/power as a new approach of human relations and generating a natural worry for the future of Earth and humankind, because all these grow as roots of some World crises, affecting, among others, the economic relations/circuits on which any sustainable progress would be based, but also the humans peaceful lives. At planetary scale, these crises and threats, first mentioning the consequences of geopolitical/military conflicts, hybrid wars, cyberattacks etc., rise a series of negative trends for states and people, as spiral of military spendings, spiral of destruction, spiral of economic losses, spiral of hate, spiral of dehumanization, spiral of fear etc., which add to the already dangerous evolutions/context of Earth ecosystem we have mentioned above (climate changes, global warming, Earth resources fading, social unbalances) and earlier [9][20]. Analysing such negative trends and the ways to mitigate them is a straight direction to identify and update the prominent, complex and dynamic factors to be continuously approached by KR. It resulted this way, by some examples (starting in 2024), dealing with unprecedented cyberattacks, as “iceberg tips” they could indicate ways to imagine and approach a part of the complex issues of KR, identifying some potential causes of World crises and threats which are linked with [2]. We noticed the danger of relativity of

evaluation of such events and trends, as depending on targets/victims assets and reliability. **These “iceberg tips” rise in fact the essential role/potential of exponential development of ICT to create benefits and vulnerabilities for the entire World, but also to defend Earth ecosystem. In the same time, it is clear that extracting and refining knowledge from these dynamic and unpredictable realities, in order to provide a sustainable progress in all areas where ICT proliferates, represent a long and complicated road which needs timely and deeper analyses.**

In the second section we have analysed some strange evolutions on the actual challenging ICT/World context, where liberty and democracy tend to be confused with disregarding or even rejecting the rule of law, logic and generally of science, without speaking of disrespect for humankind traditional values and principles, as ethics and moral ones, so often present in social media networks, where fake news, manipulation or violence are going up to hybrid war forms. **In the complex and complicate Earth ecosystem context, where humankind is evolving between apogee and survival [9], when it appears an impossibility to solve very difficult problems or further rule the turbulent World, some people believe that instead of a scientific approach they could use an intuitive/heuristic one, or instead of correct/moral behaviour they could come back to the jungle rule of force, all these because other solutions are not foreseen and unfortunately not properly searched.**

Detailing the analysis of cyber-crime domain, we could observe how deep and knowledge revealing this could be, from some examples, starting with the shocking *reference from the 1999 movie The Matrix* [4]. From the story of *Blue Pill*, we could understand the complexity of cyber-crime approaches, i.e., even the research and monitoring of this domain represent a strange mix of security real events analysis, as above presented in [2] and security virtual/vulnerability events analysis [4], further detailed and applied on the huge and emergent domain of Internet of Things (IoT). As we also presented [23][13][6], step by step we see that, with IoT, starting from home, we suddenly could be in fact at the strategical level of critical and *national infrastructures*. As if there were not enough scaring scenarios, at once we jump in the highest conflicts of the World, as it is also confirmed by [5].

Because the chances of easy proliferation of such threats are fast increasing, we believe that a realistic approach of complex processes of KR, even if using the powerful instruments and findings of ICT advances, including more and more AI, should consider, among other criteria of sustainable progress, the appropriate ethical standards. We have to observe that, in spite of the huge interest and applications fields linked with AI, the ethical standards and also the security issues are among the most difficult to improve areas of AI development, while the lack of such features has a major impact not only by the conformity point of view, but mainly on economy, by trust and reputation, as it is also approached by [7].

We have to also recall that we repeatedly [15][17][22][6] presented AI potential to request multi-criteria analyses in order to optimize the sustainable progress it would provide for the emerging challenging World, using collected data, as the example confirmed, showing *how accurately and ethically data is handled because it directly impacts system performance and user acceptance*.

Concluding, but going even beyond ethics, rules and laws, using all new data, information and knowledge from the entire Earth ecosystem, in order to learn and benefit, all these could impact individuals, companies, organizations and states, as consequently we consider that, in the actual and emerging World challenges and crises context, the role of KR is essential and mandatory to be found and implemented, as one of the most efficacious and efficient leverage to sustainable progress, everywhere humans live, scaling and spreading from individual thinking, behaviour and actions, but also reaching the incumbents and leaders of large entities.

REFERENCES

- [1]Jon Peddie,*The Evolution of Shaders - Moore's law is alive and well*, IEEE Computer Society,08/2025,<https://www.computer.org/publications/tech-news/community-voices/evolution-of-shaders>
- [2]Thomas Brewster, *The Wiretap: The Biggest DDoS Attack Ever Didn't Cause Any Noticeable Damage*, Forbes, Oct, 2024, <https://www.forbes.com/sites/thomasbrewster/2024/10/02/the-wiretap-the-biggest-ddos-attack-ever-didnt-cause-any-noticeable-damage/>
- [3]Victor Greu, *Information and communication technology is supporting people to refine knowledge as a safe balance of artificial and human intelligence could leverage the search for the right tracks of World evolution (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 16, Issue 1, Year 2025.
- [4]Bob Maley, Black Kite, Joanna F. DeFranco, *The Blue Pill Attack as a Wake-Up Call*, Jun. 2025, IEEE Computer Society, <https://www.computer.org/csdl/magazine/co/2025/06/11014253/26WXXkcgqiY?source=cedge0617>
- [5]Davey WinderNov, *Are You Already In The Matrix—35 Million Devices Under Blue Pill Attack*, Forbes,Nov, 2024, <https://www.forbes.com/sites/daveywinder/2024/11/27/is-your-router-in-the-matrix-35-million-devices-under-blue-pill-attack/>
- [6]Victor Greu, *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*,**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 4, Year 2024.
- [7]Dharani Pothula, *Enterprise-Grade Data Ethics: How to Implement Privacy, Policy, and Architecture*, IEEE Computer Society, 09/2025, <https://www.computer.org/publications/tech-news/trends/enterprise-grade-data-ethics>
- [8]Dag-Håkon Eriksen, Marta Struminska-Kutra, *Extending Knowledge, Improving Practice and Refining Values: Research Informed by the Concept of Phronesis*, February 2022, https://www.researchgate.net/publication/358633788_Extending_Knowledge_Improving_Practice_and_Refining_Values_Research_Informed_by_the_Concept_of_Phronesis
- [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]***, *AI Is Everywhere—Can Standards Catch Up?*, IEEE Computer Society Team, Published 02/03/2025,<https://www.computer.org/publications/tech-news/research/ai-standards>
- [11]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** (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 4, Issue2, Year 2013
- [12]Alex Singlaet all, *Generative AI Capturing the opportunity*, QuantumBlack, AI by McKinsey,june, 2025, <https://www.mckinsey.com/capabilities/quantumblack/how-we-help-clients?cid=other-eml-alt-mip-mck&hlkid=e3b4044e8dae4e538d3385a68bbde0a1&hctky=15934655&hdpid=766b760c-8070-4f2c-8946-b40846cea7ed>
- [13]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.
- [14]Samuel K. Moore, *How and When the Chip Shortage Will End*, IEEE Spectrum, Volume: 58, Issue: 6, Jun 2021
- [15]Victor Greu et all, *Human and artificial intelligence driven incentive-operation model and algorithms for a multi-purpose integrated crowdsensing-crowdsourcing scalable system*, Proceedings ofInternational Conference Communications 2018, (Politehnica University of Bucharest, Military Technical Academy, IEEE Romania), June 2018(COMM 2018 is covered in IEEE Explore Database and ISI Web of Science in the Conference Proceedings Citation Index).

[16]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>

[17]Florin Enache, Victor Greu, Petrică Ciofîrnae, 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)

[18]Raj Kumar Hansdah, *Scientific Progress Without True Wisdom Will Cause More Harm Than Good*, <https://www.beaninspiner.com/scientific-progress-without-true-wisdom-will-cause-more-harm-than-good>, Updated: October 21, 2021

[19]***, *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>

[20]Victor Greu, *Information and communications technologies go greener beyond IOT-behind is all the earth-Part1*, Romanian Distribution Committee Magazine, Volume 7, Issue 2, Year 2016.

[21]Amy Blackshaw, *How Cyber Resilience Enables Business Growth*, July 06,2022, https://www.bitdefender.com/blog/businessinsights/how-cyber-resilience-enables-business-growth?utm_campaign=hvi-open-source&utm_medium=email&hsmi=93802209&hsenc=p2ANqtz-9h7etfPPjDkO3RoUDsSik2A2m-MFNGagjVuij12LTXuCywRkF13zeyJANACDrIc4cX_4kowRZ22cjb0YIDQVc1SBjAtEA&utm_content=93802209&utm_source=hs_automation%2F

[22]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.

[23]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.

