Artificial Intelligence as Enabler for Sustainable Development

Ray Walshe
Adapt Research Centre
Dublin City University
Dublin, Ireland
Ray.Walshe@dcu.ie

Ansgar Koene
Senior Research Fellow
University of Nottingham
Nottingham, UK
Ansgar.Koene@nottingham.ac.uk

Sabine Baumann
Dep. Management, Information, Technology
Jade University of Applied Sciences
Wilhelmshaven, Germany
ORCID 0000-0003-1158-2897:

Massimo Panella
Dept of Information Engineering,
Electronics and Telecommunications,
University of Rome "La Sapienza", Italy
massimo.panella@uniroma1.it

Leandros Maglaras
School of CS and Informatics
De Montfort University,
Leicester,UK
leandros.maglaras@dmu.ac.uk

Francisco Medeiros
FM Tech Consult BV
Tervuren
Belgium
fm.tech.consult.@gmail.com

2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) | 978-1-6654-4963-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICE/ITMC52061.2021.9570215

Abstract*—When the UN published the 17 Sustainable Development Goals (SDGs) in 2015, emerging technologies like Artificial Intelligence (AI) were not yet mature. However, through its deployment across industry sectors and verticals, issues related to sustainability, fairness, inclusiveness, efficiency, and usability of these technologies are now priorities for global consumers and producers. This paper discusses what needs to be considered by both policy makers and 'managers' in order to exploit the use of AI for SDG achievement. AI can act as a real and meaningful enabler to achieve sustainability goals; however, it may also have negative impacts. Therefore, a carefully balanced approach is required to ensure that Artificial Intelligence systems are employed to help solve sustainability issues without inadvertently affecting other goals.

***Keywords*—artificial intelligence, sustainability, SDGs cybersecurity, standardization, green computing, data governance, Internet of Things (IoT)**

I. Introduction

In the 2021 paper by Van Wynsbergh [46], the author discusses two views of AI, AI for sustainability and sustainability of AI. Sustainable AI can be seen as a methodology and not just an application of AI. How can we develop AI technologies that are compatible with sustainability and the SDGs? Google has demonstrated that machine learning (Deepmind AI) is an effective way of leveraging sensor data to model data centre performance and improves energy efficiency by 40% [47]. Sustainable AI is as much about attitudes and values as it is about technology. Policy makers, responsible AI advocates, and AI developers should remember that there are environmental costs to AI.

In 2015, the UN launched the Sustainable Development Goals (SDGs) [1], an ambitious project to push for global improvements to be achieved by 2030. With ten years to go before the deadline, the UN has launched a "Decade of Action"[2] to accelerate progress on the SDGs. When the UN published the SDGs in 2015, emerging technologies like Artificial Intelligence (AI) were not yet mature. However, through its deployment across industry sectors and verticals, issues related to sustainability, fairness, inclusiveness, efficiency, and usability of these technologies have now become priorities for global consumers and producers [1]-[5]. AI can act as an enabler to achieve sustainability goals; however it may also have negative impacts [6]-[8].

In **section II** of this paper we review some of the most prominent ways in which AI, in combination with supporting technologies, such as Internet of Things (IoT) and Cloud Computing, can contribute towards achieving the SDGs. Based on this review we will discuss some areas of policy development that need to be addressed in order to maximize the benefits and minimize undesirable impacts.

In particular, the consumption of scarce raw materials for the production of computing and mobile devices as well as the increasing energy use of data-rich computing operations, data transfer and storage, mobile applications etc. is of considerable concern [9], [10]. **Section III** of this paper focuses on these issues under the heading of Green Computing.

Sections IV and V focus on issues surrounding the governance of AI. Calls for adaptive governance have been raised [8], [11] in order to minimize negative effects, ensure sufficient coordination and a balanced approach to achieve the UN SDGs .

Section IV addresses the role of standards for the development, deployment and use of AI, which plays an important role for establishing the required trustworthiness of the technologies that are needed for critical SDGs.

Section V focuses on the question of Data Governance, which is often a deciding factor in relation to community acceptance.

In **section VI** we turn our attention to cybersecurity, discussing potential vulnerabilities for abuse, and ways to minimize or mitigate such threats.

In this paper, we discuss some relevant aspects of AI with respect to the impact it actually has on sustainability issues for main stakeholders (i.e., policy makers, politicians, CEOs, etc.). We will introduce important topics, especially pertaining

[1] https://www.un.org/sustainabledevelopment/
[2] https://www.un.org/sustainabledevelopment/decade-of-action/

978-1-6654-4963-2/21/$31.00@2021 IEEE

to energy aspects and cybersecurity, which follow the main EU's trajectories and concern the vision of legal and ethical challenges, socio-economic impacts, and industrial competitiveness programs. This is what stakeholders usually consider to be the opportunities and challenges for work, innovation, productivity and skills.

II. AI AND UN SUSTAINABLE DEVLOPMENT

This section investigates how AI can further accelerate the achievement of UN SDGs using SDG7 (Affordable and Clean Energy), SDG8 (Decent Work and Economic Growth), SDG9 (Industry, Innovation and Infrastructure), and SDG12 (Responsible Production and Consumption) as examples because of their strong relation to industrial and manufacturing settings.

Relating to SDG9 (Industry, Innovation and Infrastructure) and SDG8 (Decent Work and Economic Growth) the use of AI systems can improve resource-use efficiency and deploy technologies and industrial processes for increased environmental sustainability. This also includes AI applications that minimize environmental impacts of logistics, for example by optimizing transport times and distances as well as through a sustainable combination of available transport modalities [12], [13].

Work environments can benefit from AI applications as automation increasingly relieves humans of routine tasks [14]-[16]. Adaptive AI applications sense whether a worker becomes tired and either provide additional support or, if necessary, gradually shut down the application so that worker safety improves. Similarly, AI can support learning processes in the work environment by adapting to individual worker needs. An experienced worker will receive less information or fewer instructions as these are disruptive for efficient work. In contrast, less experienced workers can be led through the process in a detailed step by step fashion. If the AI application detects errors it can revert to providing more guidance for the worker to remind him/her of what needs to be done. In addition, AI applications can detect muscular strain and advise workers to change their movements [14]. As robots make their way into the workforce, AI applications can be used to coordinate and steer a robot workforce. Recent experiments explored the usage of robots in a leadership position with AI applications in the role of decision maker [15],[16]. Not surprisingly, the use of AI in work environments is a highly debated topic. Recent studies found that the adoption of AI had a negative effect on worker engagement and trust [17].

Another field of intelligent systems in relation to SDG9 is to predict and prevent cyber-attacks on infrastructure. Accurate prediction assists in shielding or duplicating sensitive parts of production facilities and supply networks for higher resilience. In addition, early detection and targeted shut-down of affected sections of the infrastructure can help minimize impact (see section on cybersecurity).

Achieving SDG12 (Sustainable consumption and production patterns) and SDG7 (Affordable and Clean Energy) could also be supported by AI applications. Looking at waste generation, AI systems can reduce waste by supporting prevention, reduction, recycling and reuse [18]. End of Life (EoL) use needs to be designed into products and AI is then used to track materials and components over the product lifetime [19]. In a similar vein, applying AI can support the move from fossil fuel to renewable energy sources and improve energy efficiency.

An essential aspect to achieve sustainable consumption and production patterns lies in the ability to build and manage flexible supply chains [20]. This will also help to improve supply chain resilience in case of disruptions. AI applications allow us to model and implement sustainable supply chains, but also to trace all material and energy flows [21]. This traceability is a prerequisite to track sources of pollution and environmental damage in order to hold originators accountable.

Regarding product use, AI applications can improve customer experiences through flexibly adapting products to customer requirements and usage situations. In addition, energy usage as well as waste and pollution can be tracked and improvement measures devised and implemented [19]. AI also allows for better customer protection as producers of insufficient products can be more easily identified [22].

Although AI applications can make a positive contribution to working towards the UN Sustainable Development Goals which are related to industrial and manufacturing settings, it should be noted they can also have negative effects. In particular, the consumption of scarce raw materials for the production of computing and mobile devices as well as the increasing energy use of data-rich computing operations, data transfer and storage, mobile applications are of considerable concern [9], [10] (see also section on Green Computing).

Hence, major questions for future research related to AI and UN Sustainability Goals can be raised:

- How can AI further accelerate the achievement of UN SDGs?
- Which SDGs could benefit most from greater adopting/integration of AI technologies?
- Are current AI technologies themselves efficient and sustainable?
- How do AI developments need to be coordinated and governed to ensure a balanced approach to achieving the UN SGDs?

III. GREEN COMPUTING

AI is a key enabling technology for big data analytics in current industrial and social scenarios, where data-intensive computing has a direct impact on the existence of energy-hungry data centers. These rely on electrical systems, which play a central role in the energy transition from fossil fuels to renewables. This also involves the existence of final prosumers in everyday life, as they not only make use of computing technologies for their purposes, but also can collectively cooperate in the management of distributed energy resources as, for instance, to share energy and assets through an Smart Grid conceived as a set of renewable energy sources, loads, energy storage systems, and electric vehicles.

In this scenario, we may consider "greening by and for AI", as the latter can operate in a proactive way not only to compute green, but also to make the world green. We usually consider in green computing energy/power issues of ICT applications, such as sustainable data centers, green networking, energy harvesting, low-power electronic devices, and so on. However, by using machine learning (ML) techniques within AI we can resolve many control, decision, and optimization problems for electrical systems and Smart Grids, which involve real-time constraints and large amounts of data in very complex operation frameworks in a way that cannot be carried out efficiently by human operators.

Generally speaking, environmental effects relevant to AI should be considered for: (i) reducing the energy consumption of computers and other information systems; (ii) refurbishing and reusing old computers and equipment; (iii) designing energy efficient and environmentally sound devices; (iv) manufacturing components, computers and other systems with minimal impact on the environment. In the specific and widely considered field of deep learning (DL), computations are doubled every few months, with a dramatic increase during the latest years and a consequent large carbon footprint [21]. As a result, computational efficiency is becoming a very important criterion to be considered along with performance results of the task under investigation.

In this sense, applications can be associated with "red AI" and "green AI" solutions [22]. Red AI refers to AI algorithms that aim at the best results by using massive computational power, constrained only by economical costs. Conversely, green AI refers to solutions that are innovative and effective while maintaining or limiting the increase of computational cost, which is commonly treated as a problem constraint. This implies that green AI requires novel algorithms or physical systems for ICT and industrial applications under electrical energy and power constraints. The focus is on energy-aware design and optimization in many contexts as, for instance, big data learning, AI-based data centers, cloud computing environments, HPC and parallel computing, mobile edge and fog computing, smart cities and intelligent transport systems, sustainable building design, healthcare domains and home automation [7],[8],[11],[23].

An increasing interest is currently focused on federated or distributed ML, where computations are scaled up to networks of interconnected computing agents, which deal with information associated with multiple or geographically distributed data sources; this is the typical case of smart sensor/device networks and IoT-based networks. The particular case of IoT is interesting in the context of AI and green computing. IoT sensor devices implement a platform to collect, process, and analyze data for monitoring and controlling the cyber-physical world. Energy reduction is critical for such battery-operated devices, which also need intelligent transmission protocols that increase the life of the devices themselves [24].

AI can help to overcome the sustainability limitations of current IoT systems. Actually, the improvement of energy efficiency in IoT has to face some fundamental challenges, such as: (i) need of higher energy efficiency of the IoT network with limited bandwidth provisioning and low transmit power; (ii) advanced capabilities to release the traffic scale in the cellular networks and provide low-latency IoT services in an energy efficient manner; (iii) design of energy efficient computing platforms for IoT; (iv) lightweight security schemes for encryption to reduce the energy consumption of a secure and privacy-preserving IoT network.

Green AI and green IoT aims at reducing environmental problems in order to create a sustainable environment related to new applications of a smart and connected world. These meet the necessity to maintain climatic conditions, by introducing low-energy consumption devices or electrical appliances, minimizing gas emissions, utilizing carbon-free materials, and promoting reusability, especially in green IoT agriculture and healthcare applications [25],[26].

Overall, there are some critical questions on AI and green computing to be raised in future scientific and industrial research:

- Is the computational cost of AI algorithms and the environmental impact of the related computing resources being used as a performance measure of the considered application?
- Are the environmental effects due to the growth of data centers and to the increasing spread of IoT-based infrastructures being taken into consideration in order to prevent sustainability issues?

IV. STANDARDS

In 2017, the Technical Management Board of the International Standards Organisation (ISO) decided that the Joint Technical Committee "Information Technology" (JTC1) [27] should establish a subcommittee (SC) on Artificial Intelligence. The inaugural plenary meeting of SC42 took place in Beijing, China, in April 2018 and agreed the scope of work of SC42 as "Standardization in the area of Artificial Intelligence", specifically:

- Serve as the focus and proponent for JTC1 's standardization program on Artificial Intelligence
- Provide guidance to JTC1, IEC, and the ISO committees developing Artificial Intelligence applications

To be truly effective, AI and ML do require large amounts of data that are both diverse, trustworthy and accurate (clean). At the same time the amount of data generated is growing exponentially, particularly unstructured data created via cameras (images and videos), audio and speech recognition devices, mobile content, web pages and documents.

The EU has emerged as a regulatory leader when it comes to ethical AI by setting the stage for global standards of usability and for ensuring legal clarity in AI-based applications. Unbiased, trustworthy, ethical and gender responsive AI systems are necessary for autonomous and augmented products and services. Artificial Intelligence

978-1-6654-4963-2/21/$31.00@2021 IEEE

systems will become a core facilitator of next generation IoT, Big Data, Cloud Computing, Smart Cities, and 5G ecosystems.

- Standardization needs to evolve with the development of the technology and that certification, regulation, legislation and compliance are firmly grounded in standardization best practice.
- Inclusive and comprehensive stakeholder engagement will help reduce innovation silos, increase interoperability and help achieve a fair, transparent, diverse, safe and sustainable AI ecosystem.

As the focal point of standardization on AI within ISO and IEC, SC42's program of work looks at the entire AI ecosystem. Additionally, SC42 is scoped to provide guidance to ISO and IEC committees developing Artificial Intelligence applications. Its current program of work includes standardization in the areas of foundational AI standards, Big Data, AI trustworthiness, use cases, applications, governance implications of AI, computational approaches of AI, ethical and societal concerns.

SC42 has 21 Standards under development, including, Assessment of ML classification performance, Quality Model for AI-based systems, Data Quality Management Requirements and Guidelines, AI system life cycle processes, Risk Management, Bias in AI systems and AI aided decision making, and Overview of computational approaches for AI systems. SC42 has already published six standards, namely, in Big Data: (a) Overview and vocabulary, (b) Framework and application process, (c) Use cases and derived requirements, (d) Reference architecture, (e) Standards roadmap for Artificial Intelligence (f) Overview of trustworthiness in Artificial Intelligence.

Many unanswered questions still remain for AI and Data Standards.

- What are the architectural issues that need to be planned for successful integration of IoT, Big Data, Cloud Computing, Smart Cities, and 5G technologies?
- Where are the boundaries of recommendation, regulation, certification and legislation?
- How can standardization initiatives help create a more inclusive, fair, transparent, diverse, safe and sustainable Artificial Intelligence ecosystem?

V. DATA GOVERNANCE

Data Governance needs to be applied at all stages of the data lifecycle from generation, collection through to processing-use and storage. Data governance within organizations generally refers to who holds decision rights and is accountable for decision-making concerning data. Data governance, i.e. how to make decisions about the data, should not be confused with data management which is the actioning of the decision [28]. The explosion in the deployed number of IoT devices now makes it possible to model real world scenarios and gain insights from the Big Data generated using distributed computing architectures, such as Cloud and Edge Computing. But the research in data governance for data sharing in digital ecosystems has yet to mature.

Data protection in real-time environments is a challenge due to the flow of information and the distributed nature of the data in IoT ecosystems [29].

Typical Examples of IoT Scenarios [30] include:

- Autonomous Vehicles (AVs)
- microchip implants in farm animals,
- live data feeds of wildlife in the ocean and on land
- devices for first responders in search and rescue operations
- Smart Grid – generation, transmission, and distribution of electricity.

In these IoT Scenarios, sensors within IoT devices collect the data, and then technologies, like Edge, or Cloud Computing provide the analytics capability to extract insights from the information flow. Using the Smart Grid IoT exemplar, Data Governance issues faced by this use case are explored here.

Data governance and security are critical in Smart Grid. The development of countermeasures and techniques to detect cyber-security threats is on-going [31] with AI playing a significant role.

AI approaches like DL and ML techniques are being employed for big data collection, aggregation and data analysis for the Smart Grid. IoT devices at the edge of the network need to be secured against targeted and systemic attacks which can be directed to compromise individual devices or compromise data flows. The IoT has become embedded in the electricity network as it evolved to Smart Grid. There are governance challenges associated with IoT generated data, in the data analysis, data protection and data security aspects of this smart grid big data. The collection, use, and management of this data by AI algorithms, should follow principles that promote fairness and safeguard against race, colour, religion, sex, gender, nationality, sexual orientation, disability, or family status discrimination [9]. Data in IoT and Distributed Networks is particularly open to passive attacks or more targeted active attacks [32]. AI detection and response mechanisms can help mitigate these attacks and preserve properties of the data [33].

Data governance doesn't just apply to the design and use of the technical tools for data processing, there are also ethical concerns that need to be considered and that apply to different types of AI applications and systems. The IEEE general principles for AI and autonomous systems and human rights principles are important for the development of ethical guidelines and standards. [10] Actions taken as a result of computer algorithms and programming can be assessed according to ethical principles. For example, if a company uses an AI application to analyse general sectoral data and charges a group of people higher service charges based on variables such as gender or age, the AI application would be violating the ethical principle of equal and fair treatment.

Issues related to safety, security, ethics and trustworthiness of data and data usage are an international concern and require international organizations to engage to provide global solutions for the digital society. More research and

standardization effort is still required to answer some of the bigger questions e.g.

- What are the core principles of AI Data Governance?
- How can Data Governance help policymakers and managers understand and adopt appropriate technologies for healthcare, finance, home-living etc.?

VI. Cybersecurity

One definition of cybersecurity is: "the state of protection against the criminal or unauthorized use of electronic data or the measures taken to achieve that purpose". However, the meaning of this term is quite broad and covers protection against a multitude of threats against organizations and data. In some cases, it could be synonymous with information protection [34]. The goal of cybersecurity is to minimize successful attacks against a system (the word system can describe either a website, an operation system, an industrial control system, the internal organization network or any other facility we want to secure), while the goal of AI in security is to eliminate those attacks. However, the latter could be described as utopian, because no security mechanism will be able to achieve 100% security. Researchers and managers learn from history, incidents and mistakes that occurred in the past, in order to try to avoid them in the future. Examples of security failures have been recorded, some of which have resulted in the loss of human lives.

Here are some typical examples:

- Electricity markets managed by smart trading systems attacked [35]
- Cars with autonomous driving activated collide [36]
- Escape from a high security prison controlled by AI
- Forgery of digital signatures
- Deposits in banking systems are altered maliciously
- Fraud in the counting of electronic votes
- Credit card or mobile card cloning [37].

The most common cause of failure is during the learning phase, when the AI system does not realize exactly what it is supposed to do or detect, but finds something similar. If this remains undetected due to the similarity in AI's reactions this can lead to catastrophic consequences during deployment, e.g. non-detection of a cyber-physical attack or creation of many false positive alerts. One proposed solution would be to follow stricter tests with specific security protocols for the systems, before they enter production.

Another possible cause of failure is the fact that the number of people involved in systems development is growing rapidly. The majority of staff do not necessarily have all the knowledge required to perform appropriate tests thus leading to frequent system failures. During software development and debugging it is crucial that the program is created using reliable and secure code.

Using AI, an experimental system could theoretically be created that would be able to develop defences on its own. The idea comes from the human body that in order to deal with a virus, raises its temperature several times whilst it understands that something is wrong.

One category of solutions that combine AI and cybersecurity are self-healing mechanisms. As authors in [38] propose, along with the execution of the main process, a second process can run in parallel which is called the Healer (sub process). The job of the Healer is to check frequently the overall footprint of the operating system for possible changes. When a change is detected, it must decide whether the intervention is malicious or not, based on the training that has already been done and on the course of the system over time. Thus, the Healer will be able to detect an alteration, or a "mutation" in the code, as each change modifies the overall footprint. In addition, by checking the footprint, a backup should be made, so that in case it is decided that the change is indeed malicious, the operating system can return to a previous state where it was considered healthy. Such a method could be applied to medical systems that contain personal sensitive data. For example, the system could be checked, with the ultimate goal to find out if there is malicious use, or some software that acts as a parasite on the system.

Another group of solutions where AI meets cybersecurity Intrusion Detection Systems (IDSs). IDSs can be based on Semi-supervised learning, reinforcement learning, active learning or DL solutions [39]. According to [40], data mining, a term that is used to describe knowledge discovery, can be used as a basis in order to implement and deploy IDSs with higher accuracy and robust behaviour as compared to traditional IDSs that are based only on specific rules. The idea behind smart security mechanisms is to produce a model that either learns the normal operation of the system or creates patterns for every abnormal situation, e.g. Denial of Service Attack (DoS), Man in the Middle Attack (MITM) etc. Based on this knowledge the detection mechanism is able to detect attacks in real time [41]. The downside of using ML techniques to perform classifications is the possibility of adversaries trying to circumvent the classifiers causing misclassification [42], performing adversarial attacks.

Apart from the aforementioned adversarial attacks, AI can be used in several forms in order to perform smart attacks on systems or against specific persons, defined as artificial intelligence attacks. These smart attacks either turn AI into weapons to attack services or hack the AI algorithms used by hardware or software components [43]. Moreover, "Deepfakes" can be used to create fake news or malicious hoaxes. Deepfake ("deep learning" and "fake") is a method of synthesizing images of people based on artificial intelligence. It is used to combine and overlay existing images and videos onto source images or videos using ML techniques and can be used to deploy a social engineering attack [44] which are an essential component of Advanced Persistent Threats (APTs).

Most of the research carried out so far shows that if a system is not intelligent, it will not be able to reach a high level of security, since it must constantly learn and adapt to the circumstances. Many researchers claim that 2020 is the year of Artificial Intelligence and that by 2025 systems will have been introduced that have enough capacity and

978-1-6654-4963-2/21/$31.00@2021 IEEE
2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)

flexibility, so that they can adapt to different circumstances [45].

Based on these findings two major questions for future research related to AI and cybersecurity can be raised:

- How can AI improve cybersecurity while staying secure at the same time?
- How can we reassure that AI technology once integrated into a system is secure or improves the overall level of cybersecurity?

VII. Conclusion

Artificial intelligence systems have the capability to make a real and meaningful impact towards achieving the United Nations Sustainable Development Goals. In this article we have analyzed the current posture of AI with regard to a number of key issues such as Data Governance, Standards, Green Computing and Cybersecurity.

The analysis revealed that AI can act as a real and meaningful enabler to achieve sustainability goals; however it may also have negative impacts. Therefore, a carefully balanced approach is required to ensure that Artificial Intelligence systems are employed to help solve sustainability issues without inadvertently affecting other goals. The paper presents critical questions regarding the use of AI applications, which need to be addressed in the near future.

References

[1] M. Lahsen, "Should AI be Designed to Save Us From Ourselves?: Artificial Intelligence for Sustainability," IEEE Technology and Society Magazine, vol. 39, no. 2, pp. 60–67, 2020.

[2] A. Luers, L. Langlois, M. Mougeot, S. Kharaghani, and A. Luccioni, "Sustainability in the Digital Age [Special Issue Introduction]," IEEE Technology and Society Magazine, vol. 39, no. 2, pp. 11–13, 2020.

[3] B. v. Gils and H. Weigand, "Towards Sustainable Digital Transformation," 2020 IEEE 22nd Conference on Business Informatics (CBI), Antwerp, Belgium, 2020, pp. 104-113, doi: 10.1109/CBI49978.2020.00019.

[4] A. López-Vargas, M. Fuentes and M. Vivar, "Challenges and Opportunities of the Internet of Things for Global Development to Achieve the United Nations Sustainable Development Goals," in IEEE Access, vol. 8, pp. 37202-37213, 2020, doi: 10.1109/ACCESS.2020.2975472.

[5] Y. Shiroishi, K. Uchiyama and N. Suzuki, "Society 5.0: For Human Security and Well-Being," in Computer, vol. 51, no. 7, pp. 91-95, July 2018, doi: 10.1109/MC.2018.3011041.

[6] D. H. Fisher, "Recent advances in AI for computational sustainability," IEEE Intelligent Systems, no. 4, pp. 56–61, 2016.

[7] Y. Li, Y. Wen, D. Tao and K. Guan, "Transforming Cooling Optimization for Green Data Center via Deep Reinforcement Learning," in IEEE Trans. on Cybernetics, vol. 50, no. 5, pp. 2002-2013, 2020.

[8] J. Yang, W. Xiao, C. Jiang, M. S. Hossain, G. Muhammad and S. U. Amin, "AI-Powered Green Cloud and Data Center," in IEEE Access, vol. 7, pp. 4195-4203, 2019.

[9] Gasser, U., & Almeida, V. A. F. (2017). A Layered Model for AI Governance. IEEE Internet Comput., 21(6), 58–62. doi: 10.1109/MIC.2017.4180835

[10] The IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems" in Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems (AI/AS), IEEE, 2017, [online] Available: http://standards.ieee.org/develop/indconn/ec/ead_v1.pdf

[11] O.Y. Al-Jarrah, P.D. Yoo, S. Muhaidat, G.K. Karagiannidis and K. Taha, "Efficient Machine Learning for Big Data: A Review," in Big Data Research, vol. 2, no. 3, pp. 87-93, 2015.

[12] S. Kong et al., "Guest Editorial Introduction to the Special Issue on Intelligent Transportation Systems Empowered by AI Technologies," in IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 10, pp. 3765-3770, Oct. 2019, doi: 10.1109/TITS.2019.2940856.

[13] G. Ahmadi-Assalemi, H. M. al-Khateeb, G. Epiphaniou, J. Cosson, H. Jahankhani and P. Pillai, "Federated Blockchain-Based Tracking and Liability Attribution Framework for Employees and Cyber-Physical Objects in a Smart Workplace," 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, United Kingdom, 2019, pp. 1-9, doi: 10.1109/ICGS3.2019.8688297.

[14] S. Mavuri, K. Chavali and A. Kumar, "A study on imperative innovation eco system linkages to map Sustainable Development Goal 9," 2019 International Conference on Digitization (ICD), Sharjah, United Arab Emirates, 2019, pp. 142-147, doi: 10.1109/ICD47981.2019.9105845.

[15] J. X. Low, Y. Wei, J. Chow and I. F. B. Ali, "ActSen - AI-Enabled Real-Time IoT-Based Ergonomic Risk Assessment System," 2019 IEEE International Congress on Internet of Things (ICIOT), Milan, Italy, 2019, pp. 76-78, doi: 10.1109/ICIOT.2019.00024.

[16] N. Sahota and M. Ashley, "When Robots Replace Human Managers: Introducing the Quantifiable Workplace," in IEEE Engineering Management Review, vol. 47, no. 3, pp. 21-23, 1 third quarter,Sept. 2019, doi: 10.1109/EMR.2019.2931654.

[17] E. Mercier-Laurent, "What technology for efficient support of sustainable development?," 2015 Federated Conference on Computer Science and Information Systems (FedCSIS), Lodz, 2015, pp. 1651-1654, doi: 10.15439/2015F010.

[18] A. Pehlken, S. Baumann, "Urban Mining: Applying Digital Twins for Sustainable Product Cascade Use", 26th International Conference on Engineering, Technology, and Innovation," 2020 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Cardiff, UK, 2020, (forthcoming).

[19] S. Biller, "The operational butterfly effect: How IoT data + AI help deliver on the promise of 4IR," 2019 IEEE 15th International Conference on Automation Science and Engineering (CASE), Vancouver, BC, Canada, 2019, pp. 1-1, doi: 10.1109/COASE.2019.8843176

[20] M. Y. Morgan, M. S. El Sobki and Z. H. Osman, "Matching demand with renewable resources using artificial intelligence techniques," Eurocon 2013, Zagreb, 2013, pp. 1011-1019, doi: 10.1109/EUROCON.2013.6625105.

[21] B.E. Strubell, A. Ganesh and A. McCallum, "Energy and policy considerations for deep learning in NLP," in Proc. of ACL, 2019.

[22] R. Schwartz, J. Dodge, N.A. Smith and O. Etzioni, "Green AI," arXiv, preprint no. 1907.10597, 2019.

[23] K. Zhang, S. Leng, Y. He, S. Maharjan and Y. Zhang, "Mobile Edge Computing and Networking for Green and Low-Latency Internet of Things," in IEEE Communications Magazine, vol. 56, no. 5, pp. 39-45, 2018.

[24] S. Kallam, R.B. Madda, C. Chen, R. Patan and D. Cheelu, "Low energy aware communication process in IoT using the green computing approach," in IET Networks, vol. 7, no. 4, pp. 258-264, 2018.

[25] T. Poongodi, S.R. Ramya, P. Suresh and B. Balusamy, "Application of IoT in Green Computing," in: A. Bhoi et al. (eds) Advances in Greener Energy Technologies. Green Energy and Technology, Springer, Singapore, 2020.

[26] C. Zhang, M. Dong and K. Ota, "Enabling Computational Intelligence for Green Internet of Things: Data-Driven Adaptation in LPWA Networking," in IEEE Computational Intelligence Magazine, vol. 15, no. 1, pp. 32-43, 2020.

[27] Zielke T. (2020) Is Artificial Intelligence Ready for Standardization?. In: Yilmaz M., Niemann J., Clarke P., Messnarz R. (eds) Systems, Software and Services Process Improvement. EuroSPI 2020. Communications in Computer and Information Science, vol 1251. Springer, Cham. https://doi.org/10.1007/978-3-030-56441-4_19

[28] F. De Prieëlle, M. De Reuver and J. Rezaei, "The Role of Ecosystem Data Governance in Adoption of Data Platforms by Internet-of-Things Data Providers: Case of Dutch Horticulture Industry," in IEEE Transactions on Engineering Management, doi: 10.1109/TEM.2020.2966024.

[29] Calo, S., Bertino, E., & Verma, D. (2019). Policy-Based Autonomic Data Governance | Seraphin Calo | Springer. Springer International Publishing. doi: 10.1007/978-3-030-17277-0

[30] Poolayi, S., & Assadiyan, A. H. (2020). Governance of IoT in order to Move ahead of the calendar & live the future today. Journal of

Management and Accounting Studies, 8(3). Retrieved from http://journals.researchub.org/index.php/JMAS/article/view/877/782

[31] E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander and M. S. H. Sunny, "Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review," in IEEE Access, vol. 7, pp. 13960-13988, 2019, doi: 10.1109/ACCESS.2019.2894819

[32] Babar, S., Stango, A., Prasad, N., Sen, J., & Prasad, R. (2011). Proposed Embedded Security Framework for Internet of Things (IoT). ResearchGate. doi: 10.1109/WIRELESSVITAE.2011.5940923]

[33] 5 essential elements of Data Governance | NodeGraph. (2019, October 02). Retrieved from https://www.nodegraph.se/5-essential-elements-of-data-governance/?gclid=EAIaIQobChMI1ZWGjrHR6wIVA-vtCh3bIQCdEAAYAyAAEgI2xPD_BwE

[34] B. von Solms and R. von Solms, "Cybersecurity and information security–what goes where?" Information & Computer Security, 2018.

[35] J. Giraldo, A. Cardenas, and N. Quijano, "Integrity attacks on real-time pricing in smart grids: impact and countermeasures," IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2249–2257, 2016.

[36] E. Ackerman, "Fatal tesla self-driving car crash reminds us that robots aren't perfect," IEEE-Spectrum, vol. 1, 2016.

[37] V. Mohan, "Cell phone cloning: techniques, preventions and security measures," International Journal of Physical and Social Sciences, vol. 9, no. 7, pp. 1–11, 2019.

[38] Y. Zhao and Y. Yin, "Dynamic self-healing mechanism for transactional business process," Mathematical Problems in Engineering, vol. 2015, 2015.

[39] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 50, p. 102419, 2020.

[40] Z. Dewa and L. A. Maglaras, "Data mining and intrusion detection systems," International Journal of Advanced Computer Science and Applications, vol. 7, no. 1, pp. 62–71, 2016.

[41] L. A. Maglaras and J. Jiang, "Intrusion detection in SCADA systems using machine learning techniques," Science and Information Conference. IEEE, 2014, pp. 626–631.

[42] N. Martins, J. M. Cruz, T. Cruz, and P. H. Abreu, "Adversarial machine learning applied to intrusion and malware scenarios: a systematic review," IEEE Access, vol. 8, pp. 35 403–35 419, 2020.

[43] S.-M. Senouci, H. Sedjelmaci, J. Liu, M. H. Rehmani, and E. Bou-Harb, "Ai-driven cybersecurity threats to future networks [from the guest editors]," IEEE Vehicular Technology Magazine, vol. 15, no. 3, pp. 5–6, 2020.

[44] Ryabchuk, Natalia et al. "Artificial Intelligence Technologies Using in Social Engineering Attacks." ceur-ws.org, vol. 2654, paper 34, 2020. Retrieved from http://ceur-ws.org/Vol-2654/paper43.pdf

[45] P. Diamandis, "The world in 2025: 8 predictions for the next 10 years," Singularity University, 2015

[46] van Wynsberghe, Aimee. "Sustainable AI: AI for sustainability and the sustainability of AI." AI Ethics, 26 Feb. 2021, pp. 1-6, doi:10.1007/s43681-021-00043-6.

[47] DeepMind AI Reduces Google Data Centre Cooling Bill by 40%. https://deepmind.com/blog/deepmind-ai-reduces-google-data-centre-cooling-bill-40/