Ángel Tomás Ledo Iglesias
Researcher in training at the UNED International Doctoral School, in the "Analysis of social problems" program

THE EMERGENCE OF ARTIFICIAL INTELLIGENCE AND NOT-SO-NEW INFORMATION AND COMMUNICATIONS TECHNOLOGIES IN RELATION TO THE SECURITY OF STRATEGIC INFRASTRUCTURES
-Specific case of the electricity system-

THE EMERGENCE OF ARTIFICIAL INTELLIGENCE AND NOT-SO-NEW INFORMATION AND COMMUNICATIONS TECHNOLOGIES IN RELATION TO THE SECURITY OF STRATEGIC INFRASTRUCTURES.
-Specific case of the electricity system-

Abstract: Currently two elements stand as technological pillars of civilization. On the one hand, the sources and generation of energy, on the other hand, the information. Both elements, energy and information together with the complex technologies for its generation, management, distribution and consumption are not unrelated to security.

The new algorithms and paradigms in relation to Artificial Intelligence (AI) together with the high computing capacity achieved, have caused an irruption of AI in many areas of life. Supporting and assisting in decision-making, when not substituting in many cases already, the human decision for the decision of the machine.

This new reality becomes evident and inalienable in the management of the most complex technological systems and architectures, some of which provide essential services to the citizen.

This study aims to address different visions such as the normative, technical and technological vision, on the irruption of AI and the not so new Information and Communication Technologies (ICT), in one of the main strategic sectors, energy, specifically the electricity sector.

Resumen: En la actualidad hay dos elementos que se erigen como pilares tecnológicos de la civilización. Por una parte, las fuentes y generación de energía, por otra parte, la información. Ambos elementos, energía e información junto a las complejas tecnologías para su generación, gestión, distribución y consumo no son ajenos a la seguridad.

Los nuevos algoritmos y paradigmas en relación a la Inteligencia Artificial (IA) unido a la alta capacidad de computación conseguida, ha provocado una irrupción de la IA en muchos de los órdenes de la vida. Apoyando y asistiendo en la toma de decisiones, cuando no sustituyendo en muchos casos ya, la decisión humana por la decisión de la máquina.

Esta nueva realidad se hace patente e irrenunciable en la gestión de los sistemas y arquitecturas tecnológicas más complejas, algunas prestan los servicios esenciales al ciudadano.

Este estudio pretende abordar distintas visiones como son la visión normativa, técnica y el tecnológica, sobre la irrupción de la IA y las ya no tan nuevas Tecnologías de la Información y la Comunicación (TIC), en uno de los principales sectores estratégicos, el energético, concretamente el sector eléctrico.

Keywords: Artificial intelligence, critical infrastructures, essential services, electricity sector, cybersecurity, physical security, resilience.

Palabras clave: Inteligencia artificial, infraestructuras críticas, servicios esenciales, sector eléctrico, ciberseguridad, seguridad física, resiliencia.

1.- INTRODUCTION

Today's civilisation would be inconceivable without information, and, to a large extent, information is not conceivable without electricity. Moreover, without electricity, the supply chains of goods and services would not be possible.

If there were a large-scale power failure lasting only one week, it would cause a cascading systemic failure in the functioning of the supply chain in multiple sectors and in the provision of essential services and products. Public security would be seriously compromised. (Ledo Iglesias, 2019)

There would be no access to electronic payment methods, which would be out of service from the outset. The cash payment method would run out quickly for a large part of the population. Incidents and accidents could not be reported in real time for attention. Information and telecommunication systems would initially operate in a very precarious, limited way, powered by electrical generators fuelled by solid fuels, which would be difficult to supply and maintain for more than a few days at the level that a medium-sized urban centre would require. This is unthinkable for large cities and infrastructures or for ports, airports, stations, production centres, among others.

Access to food, water, sanitation, administration, health, and even other sources of energy. In short, all essential services would be seriously compromised, if not cancelled. This scenario would make the situation difficult for public authorities to sustain in terms of public security.

From the above, it is evident that electricity generation, distribution, access, and consumption is now a vitally important process. The entire process is taking place in the electricity sector.

The systems that enable the supply chain from production to electricity consumption are underpinned by complex technological architectures. This complexity, managed and steered by the human component, has gradually evolved towards

management with less human intervention, to the point of mere management and supervision without human consent.

In view of the importance of the electricity sector, the provision of physical and logical security in its elements and infrastructures, processes and associated services is of paramount importance.

It is in this security and in the digital transformation of the operation of the electricity system where artificial intelligence (AI) has burst in, creating a new, disruptive scenario. So much so, that it is likely to be an important factor in the emerging 4th industrial revolution.

2.- THE ELECTRICITY SYSTEM, A STRATEGIC INFRASTRUCTURE

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection is transposed into Spanish law by Law 8, 2011, of 28 April, which establishes measures for the protection of critical infrastructures (LPIC) and this in turn is developed by Royal Decree 704/2011, of 20 May, which approves the Regulation for the protection of critical infrastructures (RPIC).

It is worth mentioning that Directive 2008/114/EC has been replaced and repealed by Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities, which entered into force on 16 January and will apply from 18 October 2024, and must therefore be complied with no later than 17 October 2024.

Article 2 of the LPIC law develops the definitions for the purposes of this law, establishing that it should be understood as follows:

"Strategic infrastructure, whose operation is indispensable and cannot be replaced by alternative solutions, such that their disruption or destruction would have a serious impact on essential services", Article 2.d of the LPIC[1].

Defining an essential service as "a service necessary to maintain basic social functions, health, safety, social, and economic welfare of citizens, and the efficient functioning of state institutions and public administrations". Article 2.a of the LPIC.

Moving on from the concept of strategic infrastructure to that of critical infrastructure, as those "strategic infrastructures whose operation is indispensable and does not allow alternative solutions, so that their disruption or destruction would have a serious impact on essential services". (Ledo Iglesias & Martínez, 2020)

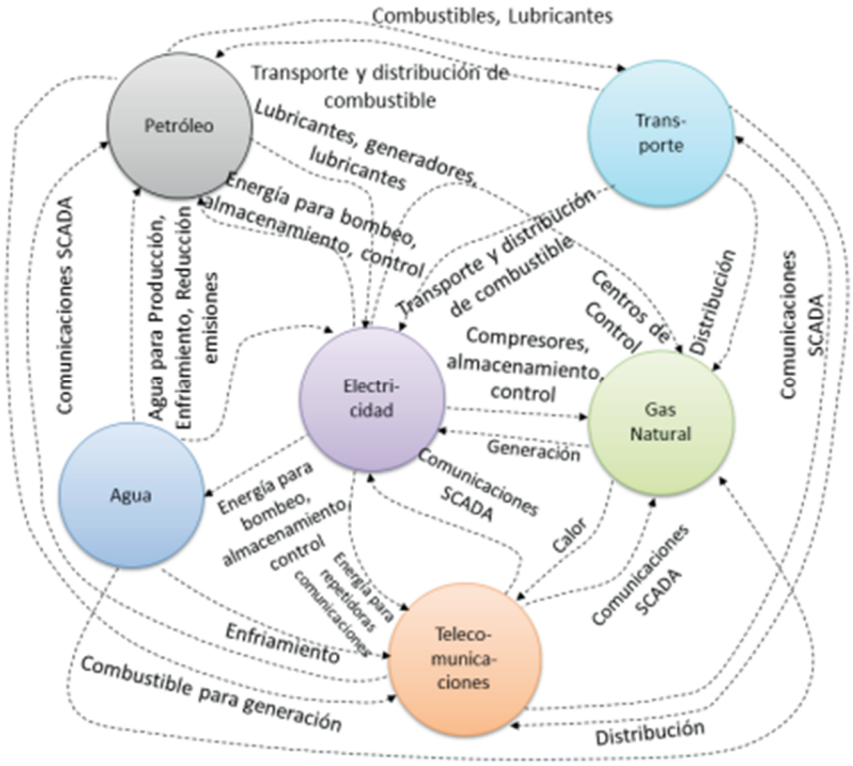
We have now identified and interrelated the concepts and natures of essential services, strategic infrastructure and critical infrastructure. Not all elements and facilities in the electricity sector are critical infrastructure; some are so because their operation is

[1] Accessible through the Official State Gazette (BOE) page at the link https://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630

indispensable and not replaceable, others may be replaced by the entry into service or supplant the provision of service by others.

It is also clearly identifiable that the set of elements, systems and facilities that operate in the electricity sector, many of them will be constituted as strategic infrastructures, due to the service they provide, already discussed above, which interacts with and depends on other strategic infrastructures and even critical infrastructures for its operation, as can be clearly inferred from image 1.

Image 1. Interdependence of the electricity sector and other critical infrastructures



*S*ource (Jaime Correa-Henao & Yusta-Loyo, 2013)

In the interest of terminological rigour and so as to avoid conceptual errors, it is necessary to clarify that within the scope of the LPIC, defined in Article 2.b, the "strategic sector as each of the differentiated areas within the labour, economic and productive activity, which provides an essential service, or which guarantees the exercise of the State's authority or the country's security. They are classified in the Annex to this regulation".

"The Spanish energy system is based on three major sectors: electricity, natural gas and oil" (Estrategia de Seguridad Energética Nacional, 2015, p. 14)

3.- EVOLUTION OF THE ELECTRICITY SUPPLY CHAIN TOWARDS A SMART GRID MODEL

The electricity system is one of the most complex systems built by man, in which the elements, subsystems and infrastructures used for the production, transport, distribution, storage and marketing of electrical energy to the final consumption points.

These processes are developed by the so-called Operational Technologies (OT) and, to manage the effectiveness and to a large extent the efficiency of their operation, more and more use has been made of Information Technologies (IT). This synergy between the OT and IT domains is no coincidence.

Traditionally, until the beginning of this century, the electricity system supply chain model was a stable and well-defined model, in which electrical energy was produced in production centres, electrical energy was transported from these production points to intermediate distribution points such as power stations and high voltage stations to other points such as medium and low voltage substations and from there to the points of consumption.

It was clear which operators were involved in each part of the process- There were some operators that produced the electricity, another operator responsible for transmission and distribution, in the case of Spain it was the company Red Eléctrica de España, and finally a series of operators that marketed it to consumers.

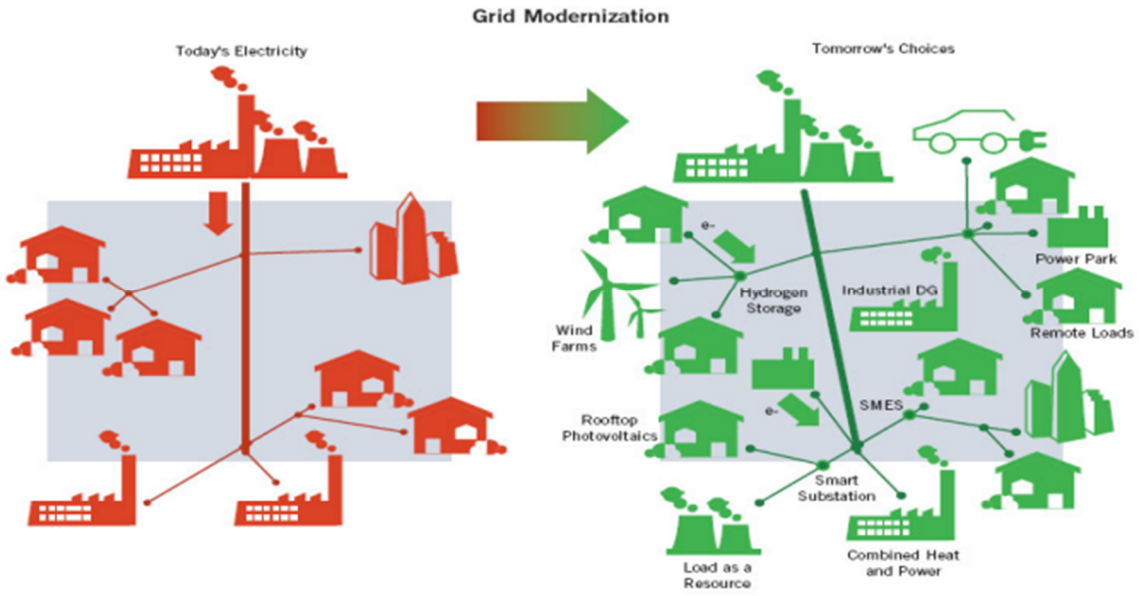
Nowadays, with developments in electricity generation sources and technologies, it is possible for many consumers to produce electricity, both for their own consumption and to inject surpluses into the electricity system to make it available to other operators.

For (Alonso et al., 2021) "New smart grids are complex cyber-physical systems in which the traditional physical systems of generation, distribution and transmission of electricity interact with the Information and Communication Technologies (ICT) used to gather measurements, communicate and process information in real time. The integration of the new cyber infrastructure with the traditional electricity infrastructure opens up new possibilities, but at the same time a number of security issues arise.

It has evolved from a system of centralised production points to a model in which production and consumption points can change dynamically, adopting both roles simultaneously or one or the other at a given time, either as producer or consumer, see Figure 2. Without prior planning or programming, in a totally dynamic and spontaneous way.

Safeguarding the stability and security of the electricity system in these new circumstances, and managing the production and consumption itself, has become an essential requirement.

Image 2. Evolution of the classic electricity production-consumption model to an intelligent electricity network or Smart Grid.



Source (Kienle & De Schryver, 2012)

The efficient electricity production model aims to ensure that whenever there is a demand for energy, there is sufficient electricity to meet that demand. However, the effective and efficient production model should aim to ensure that whenever there is a need for energy, that need it is met, but not to the extent that there is an overproduction of energy that is wasted. This is no mean feat and is almost impossible to fulfil given the number of circumstances and imponderables to be considered. Perhaps there is no wind or some of the wind farms are not working or perhaps there are not enough hours of sunshine for the photovoltaic farms to produce energy in the necessary quantities to supply mass events such as concerts, parties and even social movements that organise mass actions such switching out the lights or reducing consumption on a certain day at a certain time, etc.

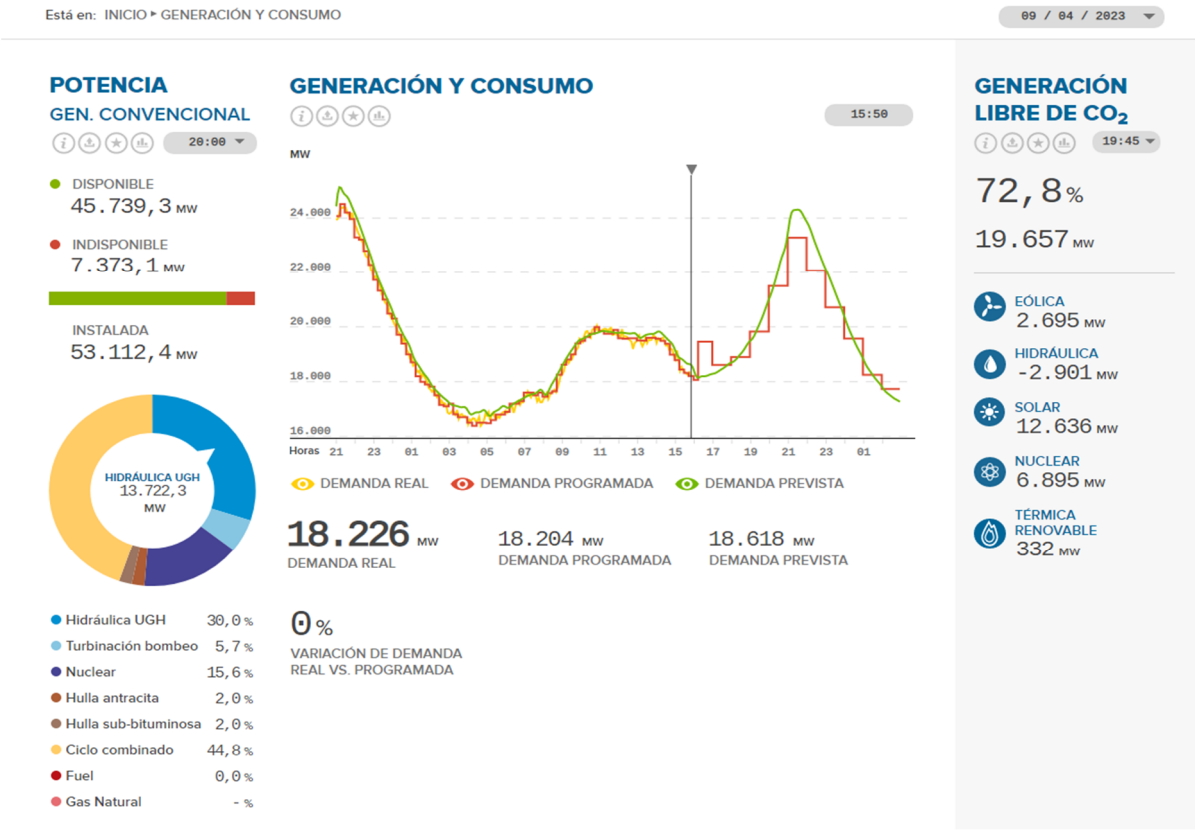
The Spanish grid is able to store an estimated of surplus energy of around 15%.

Balancing the expected electricity consumption, the electricity produced (and with which renewable sources, nuclear, etc.) and actual consumption, would be an impossible task without a high level of sensorisation of the electricity infrastructure, high calculation and processing capacity together with Artificial Intelligence techniques. This is necessary to be able to measure, analyse and react in real time to produce the necessary energy using the means of production and transport in the most economical and environmentally sustainable way possible.

This correlation between the electricity consumption measurement and requests in real time, its analysis and comparison with the estimates made, together with the reactive capacity for the production and transmission of electricity can be consulted in

real time on the website of Red Eléctrica de España[2] (REE). The result obtained on 9 April 2023 is shown in image 3.

Image: 3 Consultation production, estimated and actual electricity consumption.



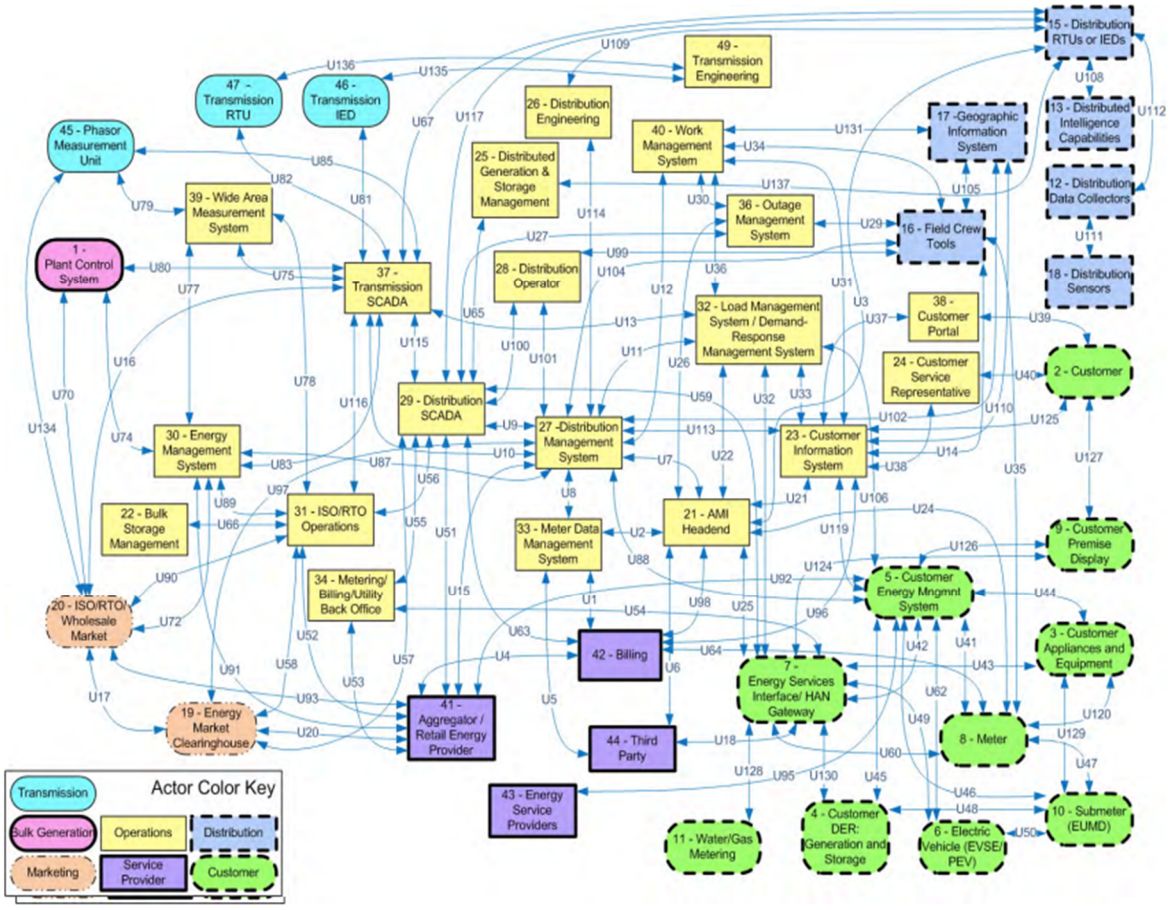
Source (REE)

4.- ARTIFICIAL INTELLIGENCE, STATE OF THE ART, CAPABILITIES AND EUROPEAN AND NATIONAL REGULATION.

The complexity of the electricity system has already been mentioned. Segmentation and automation are essential to measure the production and control parameters of the cyber-physical elements interacting in the system. A graphical representation of the different technologies involved, which interact with each other and demonstrate the complexity of the logical definition of the system, can be seen in Figure 4.

[2] https://demanda.ree.es/visiona/peninsula/nacional/total last consultation on 13 April 2023.

Image 4 Reference model of the logical interaction of systems in a smart grid.



Source (NISTIR 7628[3], p. 17)

4.1.- State of the art of AI

The huge amount of information has been generated, stored, processed and managed using emerging technologies of the industrial revolution 4.0, such as Data Mining (DM) that refers to the set of techniques and technologies aimed at exploring information in large repositories of data, not necessarily structured or stored in relational databases or Business Intelligence (BI), also known as business intelligence, which uses data mining tools, visualisation and data infrastructures and tools, oriented towards decision support. However, it is no longer sufficient because of new emerging paradigms, where the aim is no longer just to find patterns or obtain answers to specific questions, but to make use of techniques such as Big Data (BD). This term, which is standardised in the technical literature, refers to a large set of complex data and to the specific technologies in the field of ICTs for their processing.

It is necessary to be able to go beyond mere automated responses to specific events, where an already considered, identified cause has been digitised and the response procedure and action have been digitised. Thus, when presented with the same cause, the

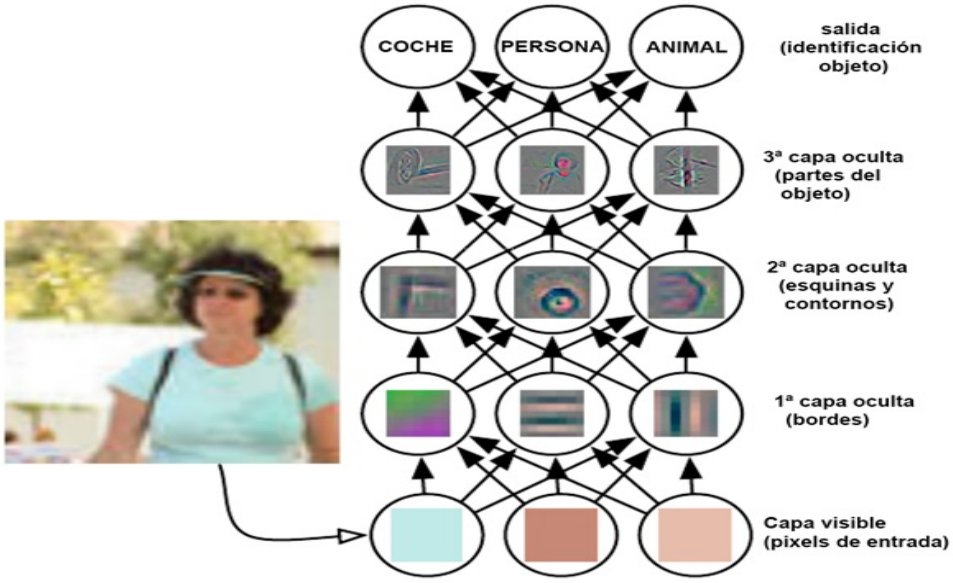
[3] Retrievable from the website https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf , last retrieved on 13 April 2023.

action will be the same, but it will not feed the system back when faced with new causes or relate them to other causes.

AI is the discipline belonging to the field of computer engineering and computer science that allows the creation of algorithms that emulate the actions that would be performed by the human mind with logical learning and reasoning. This requires the system to be able to learn by itself, using systems such as Deep Learning (DL), which uses neural networks, and Machine Learning (ML), which seeks to identify data patterns. This is how AI can emulate actions and decision-making as a human would.

Through neural networks, DL can perform actions used in technologies in the field of security, both physical and logical. It is used for biometric recognition (fingerprint, iris, veins, facial, voice), characters, texts, images, objects, among others. An example of how the object discrimination works with a neural network is shown in Figure 5.

Image 5. Object discrimination process using a neural network.



Source (Goodfellow et al., 2016)

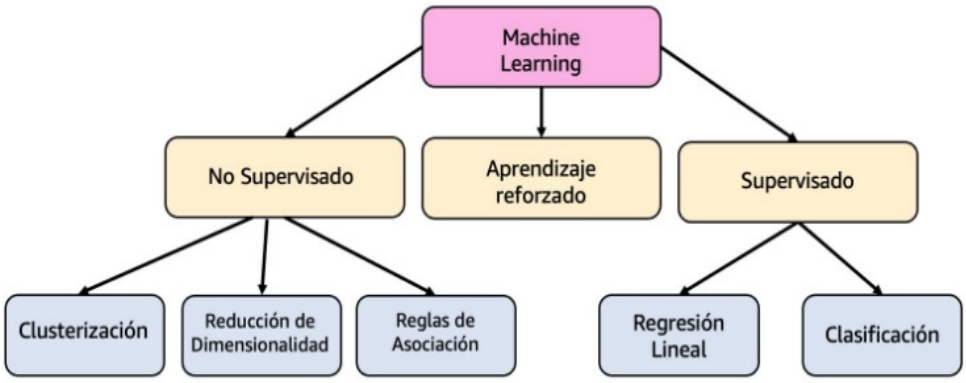
With machine learning within ML, paradigms appear that allow information to be processed and transformed into knowledge. ML uses algorithms that can be classified into three main groups for this purpose:

- Unsupervised learning. In this case, the values of the input and output variables and labels are not known. The model is trained with techniques such as clustering, association rules and dimensionality reduction.
- Supervised learning. The model is trained by using inputs from known variables and labels, it can learn from errors made, working by classification or by linear regression. It analyses relationships between inputs and outputs, teaching the algorithms the desired result for a given input. This enables it to find results even for values not previously shown to the algorithm. The process requires prolonged,

thorough and, above all, substantial training. The more examples of data use and discrimination fed into the model, the better and faster it will be learned.

- Reinforcement learning. This type of learning is based on a series of punishments, rewards that the ML agent receives for the actions it performs in its interaction with its environment. Learning the agent by exploration with its environment and the rewards it receives for its actions with the environment. (Li et al., 2021)

Image 6. ML learning techniques



Source Amazon Web Services, (aws)[4]

Humans perform some tasks instinctively. Without knowing why, we are able to intuitively recognise relationships between objects and make decisions and take consequent actions. AI, through ML, eventually finds the patterns of relationships and is able to apply them, not intuitively, but because it has found patterns. These may be absolute and probabilistic, but they are usually useful on most occasions, making AI increasingly reliable.

Supervised learning uses regression to predict a continuous value and classification predicts a class or category. Reinforcement learning teaches the AI what actions a software agent should choose in a given environment to obtain or maximise the accumulated reward. Supervised learning, on the other hand, produces knowledge with the data provided, the "inputs", without conditioning or explaining the expected outcome to the AI. In this case, the AI works by searching for similarities between inputs to find patterns and create future predictions. Inputs should not be labelled; it requires a very large amount of inputs to be able to draw conclusions.

Currently, the use of the unsupervised learning method is underutilised compared to the supervised method. However, with the improvement of algorithms and the evolution and cheapening of computing power, it can be inferred that given the cost of having a human continuously tagging information to feed the AI model with the

[4] Image retrieved from https://aws.amazon.com/es/blogs/aws-spanish/introduccion-artificial-intelligence-y-machine-learning-para-desarrollares-de-aplicaciones/ last accessed on 13 April 2023.

supervised paradigm, this will be overcome in the future in favour of the unsupervised learning model. (Salimans et al., 2016).

Unsupervised learning uses different learning techniques such as clustering, association, anomaly detection, sequence mining, dimension reduction and recommendation-based systems. (Baviera, 2017)

To achieve predictive modelling results, both these models are both programmed and training primarily with existing algorithms that are refined using the supervised machine learning paradigm. Some of the models used are "Naive Bayes[5]" classifiers or "decision trees (DT) which is a classification technique with great potential and broadly used in very different contexts, What they all have in common the need to predict the output data based on the input data. "Random forests" and "neural networks" are an improvement on the latter model[6].

4.2.- Applicability of AI to network management

Transformation and digitalisation in the electricity sector is not a recent phenomenon. Control and management elements and components are extremely expensive and have a long life cycle; some industrial control systems can be perfectly active for more than twenty years. Their replacement and automation is an ongoing process in this sector, although thousands of sensors and devices are up and running and working well, many of them highly OT oriented, as explained above.

Therefore, the degree of penetration of different technologies, including the integration of digital transformation converging IT and OT environments for its management, has been achieved through the importance of networks. Much progress has been made in the high and medium voltage networks, but less progress has been made in the "last mile" networks.

The application of AI in the electricity sector represents an improvement over traditional means of management, especially with the digitisation of the grid, and is providing intelligent integration based on very different factors, achieving the efficient convergence of old systems with new systems, optimising management. An example that has already been seen is the integration of the different factors contemplated to predict the load on the system seen in real time, becoming a critical system, as shown in image 3.

In this example, the different energy sources are visible, contributing to energy efficiency and sustainability. Another example is the EA2 project of the Instituto de Ingeniería del Conocimiento (Institute of Knowledge Engineering (IIC)) of the Autonomous University of Madrid, which provides decision-making support in wind energy production, being able to predict the weather forecast with a range of twelve to 48 hours.

[5] Based on Bayes' theorem for the calculation of probabilities of data belonging to the assigned groups according to their labels.

[6] Depending on the infrastructure, it may be of interest to use classical neural networks based on different layers, convolutional neural networks, or recurrent neural networks (Alom, Md et al, 2019).

AI will be implemented increasingly in the management and operation of the electricity grid to enable better prediction of energy consumption and production, enable decentralised control, to manage more control factors and the status of the Electrical Power System (EPS), to make the system more adaptable, robust and reliable.

The current architecture of the various production, transmission and transformation centres includes numerous measurement and control elements, incorporating intelligent electronic devices (IEDs), which are widely used throughout the electricity infrastructure, particularly in electricity substations, linked by means of the local network and globally by the interconnection of the system. This has been made possible by the advances made and by the incorporation of computer networks in this operating environment. In the past, they operated independently in each installation, but they have increasingly been incorporated into the overall structure, making use of IT, for their management by having digital remote-control terminals (RTUs). This means that there is an enormous amount of information to be managed, between measurements, commands and alarms. Having to store the data in passive storage media, and using the aforementioned Big Data and AI techniques to process it.

The introduction of intelligent agents in the control and monitoring elements has been particularly important. These comprise autonomous computational units located in the control elements of the electrical system that perform their tasks without human intervention, have their own internal control and the capacity to act in the deployed environment. They work together in coordination, reporting information and intelligence to the AI system for more unattended and efficient management. The challenge for these intelligent agents lies in modelling decision-making and designing the architecture of how they will work with the environment and with each other, giving them effective reactivity and pro-activity in the use of multi-agent systems (MAS).

The basic features of the multi-agent platform are defined by the Foundation for Intelligent Physical Agents (FIPA), now incorporated as the eleventh Institute of Electrical and Electronics Engineers (IEEE) standards committee, in 2005[7].

SMAs are widely used mainly to manage the electricity market environment with real-time control, integration of power sources and generators and overall grid operation.

4.3- Applicability to maintenance

The use of AI in system maintenance can improve network stability, reduce downtime and improve the system's entire logistics chain.

Predictive simulations of component failure can be performed to teach models what actions to take. According to Miguel Angel Fernández Céspedes, expert manager in the Renewable Energy Sector at Stratesys,

"AI improves efficiency in the renewable energy sector, reducing the cost of installation maintenance. For example, it specifies that technologies such as Machine Learning and Deep Learning make it possible to "gather information through the sensor

[7] More information can be viewed on their official website at the following link http://www.fipa.org/ , last visit on 14 April 2023.

networks located in the installations, to anticipate breakdowns and extend their useful life. The service life of the equipment is increased by anticipating possible breakdowns and reducing the number of trips by maintenance personnel to the plants. And the fact of knowing and anticipating the most recurrent breakdowns and the parts that suffer the most wear and tear reduces the stress on spare parts and the stock of less necessary ones is reduced".[8]

Some examples of implementations using AI in reactive and preventive maintenance are the "Pastora" project[9] and the Agreement between Siemens Gamesa Renewable Energy with AI and the Microsoft cloud, for preventive and corrective maintenance of rotor blades of wind turbines at wind farms[10]. The system is able to reconstitute all the photographs taken by a drone with the wind turbine stopped and view its status in 24 minutes, identifying different types of faults of varying severity, which are supervised by the technical team and eventually referred to an engineer for processing.

One notable example of the use of AI to support the maintenance of operating infrastructure in the electricity system is the BD40PEM project[11] by the Polytechnic University of Catalonia, with a budget of almost EUR 10 million, within the framework of the European Union's H2020 project, whose planned completion date is 30 June 2023. Its achievements include the detection of measurement errors, topology analysis and monitoring of low-voltage networks, as well as predictive maintenance.

4.4.- Applicability in physical security of access to SEP infrastructure.

The importance and impact of AI on the security of the operational and control (TO) elements of the SEP have already been discussed. However, it is evident that AI in physical security and access control systems, not necessarily in the electricity system, has become integrated in a cross-cutting way to all kinds of infrastructures. Nowadays, management of physical security and protection of the numerous facilities for the generation, transmission, distribution and transformation of electrical energy has been standardised and become far more efficient. It has been possible to include different private security operators, who can deploy a larger number of intrusion and sabotage detectors, facilitating the neutralisation of threats against the facilities. Recently, this has been particularly accentuated by copper theft, which apart from being economically damaging, causes significant security problems in the operation and supply of electricity.

Therefore, the use of AI in physical security systems, such as physical access control through biometrics (facial recognition, vehicles, people on white lists, people on black lists, etc.) or for managing or recognising alarms processed by the different security subsystems, to maximise the probability of detection (Pd) and in turn minimise the false alarms received (FAR index), using ML in a supervised manner, are clear examples of

[8] Obtained as a citation in the article from the website https://aserta.com.es/inteligencia-artificial-en-el-sector-energetico/ retrieved on 14 April 2023.
[9] Project led by Endesa, for the control and preventive maintenance of the distribution network, extracted from the project website https://www.endesa.com/es/proyectos/todos-los-proyectos/transicion-energetica/redes-inteligentes/pastora-inteligencia-artificial-red-distribucion , retrieved on 14 April 2023.
[10] https://news.microsoft.com/es-es/2019/04/05/siemens-gamesa-renewable-energy-crea-un-futuro-mas-sostenible-con-la-energia-eolica-la-ia-y-la-nube-de-microsoft/ , retrieved on 14 April 2023.
[11] BD40PEM, Big Data for Open innovation Energy Marketplace. Information about this project can be consulted on the project's website in the European Union, at the following link https://cordis.europa.eu/project/id/872525/es , last retrieval date 14 April 2023.

the benefits it has brought to the management and operation of security systems in electricity sector facilities.

With the digitisation of video surveillance systems, their interconnection, and the mass storage of the image in digital format and encoded on mass storage media, it has been possible, together with advances in AI and computing, to make progress in analysis, recognition and learning algorithms. Therefore, it is able to recognise objects, people and animals. These capabilities have not been limited to the field of physical security and its monitoring but have evolved to integrate information from security systems with others such as human resources, invoicing, logistics, occupational risk prevention, asset management, etc., providing high value throughout the supply chain of different systems by learning and making real time, predictive decisions.

4.5.- Contribution of AI to the cybersecurity of IT and OT systems in the electricity system.

In this paper, cybersecurity is defined as the set of policies, measures, tools and procedures to secure information and the systems in which information is stored, processed and transmitted. In a determined manner in relation to five dimensions such as confidentiality, availability, integrity, traceability, and authenticity of information.

The digitalisation of the electricity sector and how IT and OT infrastructures are converging have already been discussed, particularly since the fourth industrial revolution, in all sectors, and the electricity sector has not escaped this disruptive change. While OT systems were relatively protected by system isolation, the specificity of their systems was protected using mostly proprietary manufacturers' protocols. The emergence of telecommunications and management, coupled with the standardisation of OT systems, meant that their synergy with IT led to great productivity and a technological evolution.

The downside of this synergy is that it also inherits the threats, vulnerabilities and risks associated with IT, from which traditionally, OTs, for the above reasons, have been exempt. The interaction and synergy of IT and OTs does away with this relative security. It also disappears traumatically, because although IT have had to deal with cybersecurity problems, the strategies, policies, methods, procedures, and tools for cybersecurity are also far more mature.

OT systems lack this level of maturity, because the number of measurement and control devices is enormous and heterogeneous. They have their own protocols and characteristics that are less standardised, and with a life cycle that can extend over several decades in some cases.

Cyber-physical systems, based on control elements, such as the intelligent agents, SMAs, have other control and monitoring elements such as Industrial Control Systems (ICS). These systems encompass systems implemented in extended areas such as supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS). These systems already existed 20 years ago, but they were unable to work telematically and remotely or by interconnecting networks of centres. Nowadays, these systems have evolved to include OT measurement and control and are capable of working with intelligent control elements of IT technology, such as firewall systems (Firewire),

intrusion detection systems (IDS), intrusion prevention systems (IPS) and information and event management systems (SIEM).

In this scenario, in which a huge amount of information is generated from all the measurement and control systems of both IT and OT, AI technologies such as Big Data, Machine Learning and Deep Learning are emerging, transforming systems into expert systems with the capacity to react in real time, learn from the incidents and patterns that occur to prevent and autonomously adopt new measures that help to protect both IT and OT systems from cybersecurity attacks. Serious threats like ransomware or APTs can seriously compromise systems, in this case, the electricity sector systems.

Successful cyber-attacks have already occurred in the electricity sector, highlighting the interconnection between cyber-physical systems and how a purely computer-based attack using primarily IT has affected, and even overridden, the operation of OT infrastructures.

Cases such as the attack on the Natanz nuclear plant in Iran in April 2011 using the Stuxnet malware[12], which delayed Iran's nuclear programme by more than five years.

The attacks on the Ukrainian electricity grid in December 2015, that affected more than 225,000 people, as shown in the SANS report of March 2016, and in 2017 using the BlackEnergy malware[13] and the cyberattack on the Portuguese electricity grid, through the operator EdP[14] (Energías de Portugal, S.A.), when 10 TB of information was leaked.

In the electricity sector, a guide (Jeffrey A. Marron, Avi M. Gopstein, Nadya Bartol, Larry Feldman, 2019) to implementing a cybersecurity system in smart grids, promoted by the US government's NIST. At the national level, the guide to security in industrial protocols - Smart Grid[15], published by the National Cybersecurity Institute (INCIBE), and the guides published by the National Cryptologic Centre (CCN) are particularly interesting.

AI is being implemented in cybersecurity in different areas, such as automatic threat detection where, thanks to machine learning, systems learn and adapt to new threats and can predict future attacks with variations, performing predictive analysis, executing detection, response, and recovery actions. They are also widely used to support decision making, after acquiring and analysing thousands of signals from detection systems such as IDSs. AI continuously evolves and learns, reduces response times and detects threats earlier, providing extra time to prevent, detect and respond to cyber incidents.

[12] Detailed information on this malware can be consulted on the website of the National Cryptologic Centre, part of the National Intelligence Centre, at the following link https://www.ccn-cert.cni.es/ca/gestion-de-incidentes/lucia/23-noticias/1222-el-gusano-stuxnet-que-afecta-a-sistemas-scada-causa-revuelo-internacional.html last access on 14 April 2023.

[13] https://www.incibe-cert.es/blog/nuevo-ciberataque-red-electrica-ucrania last retrieved on 14 April 2023.

[14] News published in some security media such as the digital newspaper "CincoDías", in the following link https://cincodias.elpais.com/cincodias/2020/04/14/companias/1586887179_127560.html last accessed on 14 April 2023.

[15] Accessible from the link https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe-cert_guia_protocolos_smart_grid_2017_v2.pdf last accessed 14 April 2023.

Products like PowerMarc for protecting the email service from spam or IBM's AI-based technologies for cybersecurity adoption, such as IBM Security QRadar[16] and IBM Advisor with Watson[17] , provide comprehensive AI-based solutions for corporate cybersecurity. Data privacy classification and compliance, security profiling of user behaviour, security profiling of system performance, are other applications of AI and ML in cybersecurity.

4.6.- AI standardisation.

AI has had decades of history and evolution since it first appeared, but it is only now, with cognitive AI coming into its own, that it seems to be showing an unusual potential, which although foreseen was not recognised when it happened. The irruption of the evolution of cognitive AI has moved the thresholds of society, creating an enormous feeling of instability in relation to its impact on the current social model, and great uncertainty in relation to its true capabilities and its impact on fundamental data privacy, moral and legal rights.

On this subject, the European Union (EU) published the "White Paper on artificial intelligence - a European approach to excellence and trust", COM/2020/65 final[18] to serve as recommendations without regularly effect. A document which, although it analyses the benefits that AI will bring to all aspects of citizens' lives, recognises several potential risks such as opaque decision-making, intrusion into private lives and its use for criminal purposes. It recognises the opportunity for Europe to become a powerhouse in this field of technology, calling for coordinated action to this end and for the improvement of citizens' quality of life. It complements the framework of the European Data Strategy, where the Commission has proposed more than EUR 4 billion under the Digital Europe Programme to support it.

Following the White Paper on AI, there is now a proposal for a Regulation establishing harmonised rules on AI, known as the "AI Act"[19], which defines AI systems, identifies prohibited AI practices and risks associated with specific uses of AI, and classifies four different levels of risk: unacceptable risk, high risk, limited risk and minimal risk.

[20]At the national level, the National Artificial Intelligence Strategy[21]has been developed based on number 4 "Data Economy and artificial intelligence" of the Digital Spain Agenda 2026, which establishes strategic objectives to be achieved through six strategic axes, including aspects such as research and technological development and innovation in AI. Promotion of digital capabilities to potential national talent in AI, development of data platforms and technological infrastructures that support AI, integration of AI in the value chains of the country's economic fabric, promotion of the use of AI in public administration and in national strategic missions. Finally, an ethical and normative framework that reinforces individual and collective rights is envisaged to ensure social inclusion and well-being. (*Estrategia Nacional de Inteligencia Artificial.*2020)

---

[16] https://www.ibm.com/es-es/products/qradar-siem/addons last access on 14 April 2023.
[17] https://www.ibm.com/es-es/products/qradar-siem/addons#3071036,last access on 14 April 2023.
[18] Accessible through the link https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020DC0065,last accessed on 14 April 2023.
[19] The proposal and its annexes are available at https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence last accessed on 14 April 2023.
[20] Accessible at https://espanadigital.gob.es/sites/espanadigital/files/2022-07/Espa%C3%B1aDigital_2026.pdf last accessed on 14 April 2023.
[21] Accessible through the link https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf last accessed on 14 April 2023.

In this regard, we would mention the publication of the Extremadura Autonomous Decree-Law on AI, (Decreto-ley 2/2023, de 8 de marzo, de medidas urgentes de impulso a la inteligencia artificial en Extremadura. 2023) as a regional regulation. With objectives such establishing AI that is ethical, reliable and respectful of fundamental rights, increasing technical training in AI, promoting the implementation of AI in companies in the region, among others. In its first additional provision, it establishes the drafting and approval of an Artificial Intelligence Strategy for Extremadura.

5.- CONCLUSIONS AND FUTURE LINES OF RESEARCH

Throughout this article, it has been possible to identify the electrical system as one of the most complex systems, if not the most complex system devised and built by man. The importance of the electricity sector as a vital component of today's society has been explained, concluding that the electricity sector is a part of the country's strategic infrastructures and that some are critical infrastructures, seeing how its affectation would have a cascading impact on strategic infrastructures in almost all strategic sectors.

The digital transformation and the confluence of IT and OT in electricity systems were explored in depth, illustrating the development of the traditional production-transport-consumption model of electricity towards smart power grid systems, the so-called Smart Grids,

The evolution in the number of detectors generating signals and data, together with advances in the capabilities of computer networks and computing capacity, have encouraged the integration of increasing synergy and interoperability between IT and OT, with AI emerging as an indispensable part of the solution to the management, maintenance, and governance of the electricity system. Exploring the applicability of AI in these processes.

We have also explored the relationship between AI and cybersecurity systems, its implications and possibilities for implementation and exploitation in relation to the electricity sector.

Finally, we have identified the main regulations and regulatory initiatives both at the European and national level, with a particular case of development and regulatory proposal at regional level, such as the development of Decree Law 3/2023 of the Regional Government of Extremadura. These reveal the concerns and hopes that the European Union and Spain have about AI and its emergence and impact on the lives of citizens and institutions.

The upcoming Artificial Intelligence Regulation (known as the "AI Act"), together with the European Data Protection Regulation (EDPR), will be the de facto global standards for AI governance.

Based on the initial steps outlined in this work, several lines of future research emerge, regulatory, ethical, technical, technological, and social, on AI and more specifically in the electricity sector. Cybersecurity research in cyber-physical environments and the adoption of multivariate risk analysis, administrative, civil, and criminal investigation of fraud and malpractice in the use of AI for both electricity service provision and fraud and other pernicious effects on the system are proposed.

BIBLIOGRAPHY

- Alonso, M., Turanzas, J., Amaris, H., & Ledo, A. T. (2021). Cyber-physical vulnerability assessment in smart grids based on multilayer complex networks. *Sensors, 21*(17), 5826.
- aws. *Innovar con el uso de machine learning.* Amazon Web Service (aws). Retrieved 14/04/2023, from https://aws.amazon.com/es/ai/
- Baviera, T. (2017). Técnicas para el análisis del sentimiento en Twitter: Aprendizaje Automático Supervisado y SentiStrength. *Dígitos, 1*(3), 33-50.
- Decreto-ley 2/2023, de 8 de marzo, de medidas urgentes de impulso a la inteligencia artificial en Extremadura. Decreto LeyU.S.C. (2023). https://www.boe.es/buscar/act.php?id=BOE-A-2023-8795&p=20230310&tn=6
- *Estrategia Nacional de Inteligencia Artificial.* (2020). (). https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT press.
- Jaime Correa-Henao, G., & Yusta-Loyo, J. M. (2013). *Seguridad Energética y Protección de Infraestructuras Críticas.*ssn: 2145-4086
- Jeffrey A. Marron, Avi M. Gopstein, Nadya Bartol, Larry Feldman. (2019). *NIST-Cybersecurity Framework Smart Grid.* (). https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2051.pdf
- Kienle, F., & De Schryver, C. (2012). 100% green computing at the wrong location?
- Ledo Iglesias, A. T.Analysis of Social and Legal Issues on Critical Infrastructures in Spain. Paper presented at the *2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG),* 375-377.
- Ledo Iglesias, A. T., & Martínez, M. A. (2020). El sistema eléctrico español como infraestructura crítica: su protección ante ciberincidentes. *Cuadernos De La Guardia Civil: Revista De Seguridad Pública,* (61), 97-126.
- Li, X., Shi, J., & Chen, Z. (2021). Task-Driven Semantic Coding via Reinforcement Learning. *IEEE Transactions on Image Processing : A Publication of the IEEE Signal Processing Society, 30*, 6307-6320. 10.1109/TIP.2021.3091909
- Salimans, T., Goodfellow, I., Zaremba, W., Cheung, V., Radford, A., & Chen, X. (2016). Improved techniques for training gans. *Advances in Neural Information Processing Systems, 29*