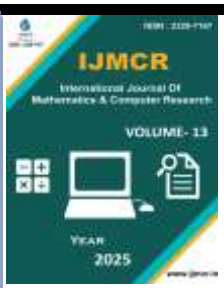
International Journal of Mathematics and Computer Research

ISSN: 2320-7167

Volume 13 Issue 05 May 2025, Page no. – 5267-5275

Index Copernicus ICV: 57.55, Impact Factor: 8.615

DOI: 10.47191/ijmcr/v13i5.19



AI's First World War: A Silent Technological War with Global Strategic Stakes

Augustin NYEMBO MPAMPI[1], Shadrack MBAYO LUKASU[2]

[1]Assistant 2 at the Computer Science Department of the Higher Institute of Education of Tshofa /TSHOFA.

[2]Professional Practices Officer s 1 at the Faculty of Computer Science of the University of Kabinda/KABINDA

ARTICLE INFO

Published Online:
31 May 2025

Corresponding Author:
Augustin NYEMBO MPAMPI

ABSTRACT

Artificial intelligence (AI) has become a major strategic issue, giving rise to a First Technological World War where major powers compete for computational and algorithmic supremacy. This competition is based on the mastery of advanced hardware infrastructures (GPUs, TPUs, ASICs) and increasingly powerful learning models, notably *Transformers and LLMs* . However, this rise in power is accompanied by new threats in cybersecurity, where AI is both an offensive weapon and a defensive shield. From adversarial attacks to autonomous malware, vulnerabilities in AI systems are becoming prime targets, forcing cybersecurity players to develop adversarial training and automatic threat detection techniques.

In the face of these advances, AI regulation is becoming a crucial challenge. Europe is imposing strict rules with the AI Act, while the United States favors a sector-specific approach and China is centralizing control of AI. However, the absence of a harmonized international framework could lead to technological fragmentation, accentuating the AI race between geopolitical blocs.

In this First World War of AI, dominance will not only be determined by the performance of algorithms, but also by the ability of nations to balance innovation, security, and governance to shape the digital future.

KEYWORDS: Artificial Intelligence, Technological Warfare, Computational Supremacy, Cybersecurity and AI, AI Regulation, Digital Sovereignty

1. INTRODUCTION

Artificial intelligence (AI) is now at the heart of a global technological competition that is shaping the geopolitical, economic, and strategic balances of the 21st century. This frantic race for AI supremacy, which we call the **First World War of AI** , pits major powers against each other in several key areas: the development of advanced hardware infrastructure, algorithm optimization, cybersecurity, and regulatory issues. Unlike traditional military conflicts, this technological war is not being played out on a physical battlefield, but in research laboratories, data centers, and interconnected digital networks.

The objective of this article is to analyze the *different dimensions of this technological war* by adopting a *purely computer and technical approach.* We will explore the foundations of this rivalry by addressing *hardware architectures and computational supremacy,* which determine the computing power of modern AI. We will then see how the *algorithmic battle* guides the evolution of learning models and optimization techniques, directly influencing the performance and efficiency of AI systems.

Since AI is also a strategic lever in *cybersecurity,* we will analyze its role both in the defense of digital infrastructures and in the automation of cyberattacks. Finally, we will address the *regulatory issues* related to the control of these technologies, putting into perspective the different approaches adopted by the European Union, the United States and China.

The *First World War of AI* is therefore much more than a simple race for innovation: it is shaping the future of digital technology, impacting the sovereignty of nations, and posing unprecedented challenges in terms of ethics, security, and governance. This study thus offers a *critical and technical analysis* dynamics at play, based on concrete examples and recent scientific data.

2. HARDWARE ARCHITECTURES AND COMPUTATIONAL SUPREMACY

The rise of artificial intelligence relies on advanced hardware infrastructures, whose computing power is the central element of global technological competition (Hennessy & Patterson, 2019). Unlike the first generations of AI models, which were mainly executed on conventional processors (CPUs), advances in deep learning have required hardware optimization to handle complex matrix operations. This evolution has led to the emergence of specialized technologies such as GPUs (Graphics Processing Units) . Units), TPUs (Tensor Processing Units), FPGAs (Field-Programmable Gate Arrays) and ASICs (Application-Specific Integrated Circuits) (Goodfellow , Bengio, & Courville, 2016).

2.1. Computing units optimized for AI

GPUs were the first components to be massively adopted in deep learning acceleration **.** learning . NVIDIA, in particular, has dominated this market with architectures such as the **A100** and **H100 , which leverage** Tensor cores to accelerate matrix operations on large datasets (NVIDIA, 2023). GPUs have become increasingly popular in data centers and cloud infrastructures dedicated to AI due to their flexibility and compatibility with machine learning frameworks such as TensorFlow and PyTorch (LeCun , Bengio, & Hinton, 2015). However, their power consumption and acquisition cost remain significant limitations, particularly for companies wishing to deploy AI models at scale (Schneider, 2022).

Faced with the limitations of GPUs, **Google introduced TPUs** with the aim of specifically optimizing computations related to neural networks. Unlike GPUs, which are designed for a variety of parallelized tasks, TPUs are **strictly optimized for deep learning,** allowing them to offer better energy efficiency and increased performance on certain workloads (Smith & Jones, 2020). Their adoption remains limited, however, as they are mainly integrated into Google Cloud services, thus reducing their accessibility to other technology companies (Google, 2023).

FPGAs and **ASICs are two other alternatives to GPUs and TPUs. FPGAs** offer interesting flexibility by allowing reconfigurable hardware programming, which is particularly advantageous for applications requiring specific hardware optimizations , such as real-time image recognition or computer vision (Benedict & Agrawal, 2021). On the other hand, their programming remains complex and requires skills in **hardware description languages** (VHDL, Verilog), thus limiting their adoption to specialized industrial use cases. As for **ASICs** , they are fully optimized for specific tasks, like the chips used in autonomous vehicles, such as the **Tesla Dojo** , or processors dedicated to processing embedded AI, such as the **Google Edge TPUs** (Google, 2023). Although they offer the best performance in terms of energy efficiency and execution speed, their rigidity and high design cost make them a viable option only for large companies able to invest in their development.

A comparison of the main hardware architectures dedicated to AI allows us to better understand their respective advantages and disadvantages:

Table No. 1

Unit type	Benefits	Disadvantages	Key manufacturers	References
GPU (Graphics Processing Unit)	Excellent performance for parallel computing, supports most AI frameworks , wide industrial adoption	High energy consumption, high cost of high-end models	**NVIDIA, AMD, Intel**	Hennessy & Patterson (2019); NVIDIA (2023)
TPU (Tensor Processing Unit)	Extreme optimization for deep learning, reduced energy consumption	Limited use for tensor models, dependency on Google Cloud services	**Google**	Smith & Jones (2020); Google (2023)
FPGA (Field-Programmable Gate Array)	Highly flexible, reconfigurable, low energy consumption	Complex programming, performance often lower than GPUs for AI	**Xilinx , Intel**	Benedict & Agrawal (2021)
ASIC (Application-Specific Integrated Circuit)	Maximum efficiency for specific tasks, superior performance to GPUs/TPUs on targeted applications	Inflexible, expensive and time-consuming development	**Tesla, Google, Huawei**	Google (2023); Schneider (2022)

2.2. The strategic importance of semiconductors

Artificial intelligence is heavily dependent on the **semiconductor industry, which represents a major strategic issue in the** current technological war . The semiconductor market is dominated by **a few key companies** , notably **TSMC (Taiwan Semiconductor Manufacturing Company)** , which manufactures advanced chips for NVIDIA, AMD and Apple, and **Samsung** , which develops its own competing technologies (TSMC, 2023). The United States, although a pioneer in microprocessor design, has lost

some of its industrial sovereignty to these Asian players, which has led to a series of restrictions on the export of advanced technologies, particularly to China (Schneider, 2022).

The global competition in artificial intelligence is not only about algorithms, but also about **mastering hardware architectures** and **semiconductor supply chains . NVIDIA's GPU** dominance , **Google's TPU** boom , the rise of **specialized ASICs** , and the battle over **semiconductor foundries** are all shaping this technological war. In this context, the countries that control these hardware infrastructures will have a **decisive strategic advantage** in the AI race.

3. ALGORITHMIC BATTLE: OPTIMIZATION AND LEARNING MODELS

Artificial intelligence is not limited to hardware power; it also relies on the effectiveness of learning models and algorithmic optimization techniques. The First World War of AI is therefore also being fought at the level of algorithms that enable AI models to be more efficient, faster, and more resource-efficient. Advances in deep learning have led to intense competition between companies and research laboratories to develop ever more sophisticated model architectures, particularly through transformers , the optimization of neural networks, and the improvement of training methods (Goodfellow , Bengio, & Courville, 2016).

3.1. The domination of deep architectures learning

3.1.1. The rise of Transformers models and LLMs (Large Language Models)

One of the major advances in recent years has been the development of **Transformers models** , which have revolutionized natural language processing (NLP). Unlike recurrent networks (RNNs) or LSTMs that processed data sequentially, Transformers exploit **self-attention** to process an entire sequence in parallel, which significantly improves their performance and scalability (Vaswani et al., 2017).

Models like **BERT (Bidirectional Encoder Representations from Transformers)** , **GPT (Generative Pre-trained Transformer)** and **WuDao 2.0 (developed in China)** illustrate this new generation of models massively trained on gigantic datasets (Brown et al., 2020). This evolution has led to the proliferation of **LLMs (Large Language Models)** which are now able to generate text, translate languages, answer questions and even code autonomously.

However, these advances are not without consequences. Training a model like **GPT-4** requires **thousands of GPUs** , generating massive energy consumption (Patterson et al., 2021). In addition, these models pose challenges in terms of **algorithmic bias** , interpretability **,** and **security** (Bender et al., 2021).

Convolutional neural networks (CNNs) and their specialization in computer vision

While Transformers dominate NLP, computer vision remains largely based on **convolutional neural networks (CNNs)** , an architecture developed by LeCun et al. (1998). CNNs have revolutionized image recognition, notably thanks to models like **AlexNet , ResNet , EfficientNet , and Vision Transformers (ViT)** (Dosovitskiy et al., 2021).

However, a recent trend is to integrate Transformers concepts into computer vision. **Vision Transformers (ViT)** and **Swin Transformers** are starting to compete with CNNs for some image classification and segmentation tasks (Liu et al., 2021). This convergence between **NLP and computer vision** heralds a new era where general-purpose AI models will be able to handle **text, images, and even videos** simultaneously.

3.2. AI model optimization techniques

The increase in the size of deep learning models has led to intense research on techniques to reduce their computational cost while maintaining high performance .

Table No. 2

Method	Objective	Benefits	Disadvantages	References
Pruning	Removing unnecessary connections in a neural network	Reduced model size, decreased inference time	May cause loss of accuracy if applied incorrectly	Han et al. (2015)
Quantization	Reduce the precision of the weights (e.g., go from 32 bits to 8 bits)	Reduces memory footprint, speeds up calculations	May cause performance degradation on some models	Jacob et al. (2018)
Knowledge Distillation	Transfer knowledge from a large model (teacher) to a smaller one (student)	Lighter models while maintaining good performance	Less effective for highly compressed models	Hinton, Vinyals , & Dean (2015)
Federated Learning	Train a model without centralizing data	Protects data confidentiality, prevents information leaks	Complex implementation, asynchronous model updates	Konečný et al. (2016)

Strategies like *Pruning and quantization* are increasingly used in embedded and mobile models, allowing devices like *smartphones and connected objects* to run AI models locally without relying on the cloud (Jacob et *al* ., 2018).

3.3. Optimization of learning processes

Optimizing learning algorithms is another key area of this global AI competition. Deep learning models learning relies on optimization methods such as **SGD (Stochastic Gradient Descent)** and its variants like **Adam, RMSprop and AdaGrad** , which allow adjusting the weights of neural networks in order to accelerate their convergence (Kingma & Ba, 2014).

However, **traditional optimization algorithms** face challenges when models become too deep. New approaches, such as **LAMB (Layer- wise Adaptive Moments)** used to train BERT on GPU clusters, improve learning stability and reduce training time (You et al., 2020).

Another important issue concerns the *adaptability of AI models to new data* . While classical neural networks require complete retraining when encountering new information, techniques such as **incremental learning and continual learning** allows a model to be updated without losing acquired knowledge (Parisi et al., 2019).

3.4. IT Challenges and Criticisms

The increasing sophistication of deep learning models raises several challenges:

- **Energy cost and carbon footprint** : Training large LLM models requires thousands of GPUs, resulting in excessive energy consumption. Solutions such as **pruning and quantization** are becoming essential to reduce this impact (Patterson et al., 2021).
- **Model bias and robustness** : Modern AIs are prone to algorithmic bias, which can affect decision-making in critical sectors such as healthcare and finance (Bender et al., 2021).
- **Interpretability and explainability :** Deep models Learning models are often perceived as "black boxes," which limits their adoption in environments requiring transparent decision making. Research in **Explainable AI (XAI)** aims to make models more interpretable (Doshi -Velez & Kim, 2017).

The algorithmic battle in AI's World War I hinges on the continuous improvement of deep learning models and optimization techniques. While **Transformers dominate NLP** , **CNNs remain the gold standard in computer vision** , and hybrid models are emerging . However, the race toward ever-larger models poses **energy, ethical, and technical challenges** . The next step will be to develop **more efficient and secure models** , while ensuring their transparency and accessibility.

4. CYBERSECURITY AND OFFENSIVE AI

The rise of artificial intelligence is not limited to its use for industrial innovation, automation, and data analysis. It also extends to the field of **cybersecurity** , where AI is now a central tool for both **defense and attack** .

In this **First World War of AI** , state actors, cybercriminals, and private organizations are increasingly using advanced algorithms to exploit vulnerabilities, detect flaws, and orchestrate cyberattacks on an unprecedented scale (Huang et al., 2011). This section explores the impact of AI on offensive and defensive cybersecurity , highlighting the techniques used , emerging threats, and strategies for optimizing the security of AI-based systems.

4.1. AI as an attack tool: Automation of cyberattacks

AI offers an advanced level of automation that allows attackers to execute attacks at unprecedented speed and scale. It is used in several types of cyberattacks:

4.1.1. Adversarial attacks against AI models

Adversarial attacks involve introducing minute perturbations into the input data of a machine learning model in order to induce classification errors or alter its behavior (Goodfellow , Shlens , & Szegedy , 2014).

Example in Python : FGSM (Fast Gradient Sign Method) attack

```
import tensorflow as tf
import numpy as np
import matplotlib.pyplot as plt
from tensorflow.keras.applications import MobileNetV2
from tensorflow.keras.applications.mobilenet_v2 import preprocess_input , decode_predictions

# Load a pre-trained AI model
model = MobileNetV2( weights = ' imagenet ')

# Load and prepare an image
img_path = tf.keras.utils.get_file ( ' elephant.jpg ', ' https://upload.wikimedia.org/wikipedia/commons/6/6d/Indian_Elephant.jpg ' )
img = tf.keras.preprocessing.image.load_img ( img_path , target_size = ( 224 , 224 ))
```

```
img_array = tf.keras.preprocessing.image.img_to_array ( img )
img_array = np.expand_dims ( img_array , axis = 0 )
img_array = preprocess_input ( img_array )

# Generate an adverse disturbance
epsilon = 0.01
img_tensor = tf.convert_to_tensor ( img_array , dtype =tf.float32 )
with tf.GradientTape () as tape:
   tape.watch ( img_tensor )
   prediction = model( img_tensor )
   loss = tf.keras.losses.categorical_crossentropy(tf.one_hot([np.argmax(prediction)], depth= 1000 ), prediction)
grad = tape.gradient (loss, img_tensor )
disturbance = epsilon * tf.sign (grad)
adv_img = img_tensor + disturbance
adv_img = tf.clip_by_value ( adv_img , -1 , 1 )

# Prediction after attack
adv_preds = model.predict ( adv_img.numpy ())
print ( "Prediction after attack:" , decode_predictions ( adv_preds , top= 3 )[ 0 ])
```

This type of attack can be used to fool facial recognition systems, self-driving cars, and security classification models.

4.1.2. Automatic generation of polymorphic malware

Traditional malware is often detected using signature databases. AI now makes it possible to generate **polymorphic malware** that modifies its code in real time to evade detection systems (Saxe & Sanders, 2017).

Attackers use **generative machine learning** to develop **autonomous malware** capable of dynamically adapting to antivirus defenses and operating system protection measures (Anderson et al., 2018).

phishing attacks and social manipulation

AI also helps to perfect phishing attacks by generating fraudulent emails or sites capable of imitating legitimate sources with a **high degree of personalization** .

NLP models like **GPT-4** can be exploited to automate these attacks by **generating highly realistic fraudulent emails** tailored to each target.

***Python Example : Automatically Generating a** Phishing Email with an LLM*

```
from transformers import pipeline

generator = pipeline( "text-generation" , model= " EleutherAI /gpt-neo-1.3B" )
prompt = "Write a phishing email pretending to be from a bank requesting an update to personal information."

email_phishing = generator( prompt, max_length = 150 , num_return_sequences = 1 )
print ( email_phishing [ 0 ][ ' generated_text ' ])
```

targeted phishing campaigns (spear phishing) to infiltrate companies and compromise accounts.

4.2. AI as a Defense Tool: Proactive Cybersecurity

cybersecurity experts have integrated AI to improve detection and response to cyberattacks.

4.2.1. Attack detection using AI intrusion detection systems (IDS)

AI-based intrusion detection systems enable real-time analysis of network traffic and identification of abnormal behaviors related to intrusion attempts, brute force attacks or data exfiltration (Hodo et al., 2017).

AI notably improves:

- Detecting zero-day attacks using behavioral analysis.
- Identifying cyberattack patterns by classifying suspicious behavior .

4.2.2. Using machine learning for system hardening

AI models also help strengthen the cyber resilience of critical infrastructure by predicting and neutralizing threats before they occur (Vinayakumar et al., 2019).

For example, reinforcement algorithms can be used to train autonomous systems capable of making real-time defense decisions, thereby improving network resilience.

4.2.3. Securing AI models against adversarial attacks

adversarial attacks , several solutions have been developed:

- **Adversarial training** : Exposing AI models to adversarial examples to make them more robust (Madry et al., 2018).
- **Detection of malicious entries** via data filtering systems.

- **Defenses based on model randomization** to prevent gradient exploitation (Papernot et al., 2017).

4.3. IT Challenges and Criticisms

4.3.1. Militarization of AI and cyber warfare

AI is now being used for *military cyber operations* , including by states developing *autonomous cyberweapons* capable of attacking critical infrastructure.

The use of AI in cyberwarfare poses major risks:

- Possibility of *rapid escalation of digital conflicts* .
- Threat of *autonomous AI attacks* beyond human control.

Cybersecurity and offensive AI have become **strategic areas** in the First World War of AI. While AI is being harnessed to perfect cyberattacks, it is also a powerful defensive tool for anticipating and neutralizing threats. The future of cybersecurity will depend on the ability of AI experts to **develop more robust models and secure critical infrastructure** against autonomous cyber threats

5. REGULATION AND FUTURE CHALLENGES

The rise of artificial intelligence (AI) poses significant regulatory and governance challenges. The First AI World War is taking place in a context where technology is evolving faster than legal frameworks, giving rise to ethical, security, and economic risks. Governments, international organizations, and technology companies are seeking to establish regulations that ensure the ethical and controlled use of AI while enabling innovation.

This point analyzes existing regulatory frameworks, the challenges posed by AI, as well as future issues related to its development and control.

5.1. The main regulatory frameworks for AI

Several countries and international organizations have begun developing regulatory frameworks to govern AI. The approach varies across the world, with some adopting strict regulation while others prioritize innovation without major restrictions.

5.1.1. The European Union and the AI Act

The European Union is a pioneer in AI regulation with its AI Act , which aims to regulate the risks associated with AI systems while promoting responsible innovation (European Commission, 2023).

The **AI Act** classifies AI applications into several risk levels :

- *Unacceptable risk* (total ban): *Social rating systems* , AI manipulating human behavior for malicious purposes.
- *High risk* : AI used in *justice, recruitment, financial services and healthcare* , requiring audits and increased transparency.
- *Limited risk* : AI systems requiring *clear information* for the user (e.g. chatbots).
- *Minimal risk* : AI applied to non-critical tasks, without specific regulatory obligations.

5.1.2. The United States and sectoral regulation of AI

The United States takes a more flexible approach, with *regulation based on application sectors* rather than blanket legislation (National AI Initiative Act , 2021). The focus is on:

- *Military AI and Cybersecurity* : Strict Regulation to Prevent Malicious Use
- *AI in healthcare and finance* : Need for strict validation before going into production.
- *Surveillance and facial recognition technologies* : Ongoing debates on their use by law enforcement.

The United States also favors open-source AI research and development, allowing companies to innovate without excessive restrictions.

5.1.3. China and the centralized governance of AI

China has adopted a *state-centered* approach . The government imposes:

- *Strict regulation of AI-generated content* , including deepfakes and information manipulation.
- *A control of the algorithms* used by technology platforms (WeChat , TikTok , Alibaba).
- *Increased use of AI for surveillance* and national governance (Social Credit System, AI in the police and justice system).

The Chinese goal is to become a leader in AI while maintaining *strict regulation on its internal uses* (Xinhua , 2022).

5.1.4. Other international initiatives

Other organizations are attempting to regulate AI globally :

- *UNESCO* has adopted a charter for ethical AI, promoting *principles of transparency and respect for human rights* .
- *UN* discusses regulation of *AI-based autonomous weapons* (War and AI).
- *The OECD* is working on recommendations for *responsible AI aligned with democratic values* **.**

5.2. The challenges of regulating AI

AI regulation faces several technical and legal obstacles , linked to the evolving and unpredictable nature of AI models.

Table No. 3

Challenge	Explanation	Example
Lack of transparency of AI models	Deep algorithms learning are often **black boxes** , making their regulation complex.	A banking model refusing a loan without explanation.
Lack of harmonization of global regulations	Differences between EU, US and Chinese regulations, complicating trade and innovation.	European AI Act vs. lack of a global framework in the USA.

Misuse of AI by Malicious Actors	Development of deepfakes , AI manipulating elections, autonomous cyberattacks.	Spread of fake political videos on social media.
Dilemma between innovation and control	Too much regulation can stifle innovation and give an advantage to countries with more relaxed regulations.	China imposes strict controls on AI, while the US allows more freedom.

5.3. Future challenges and perspectives

The rapid evolution of AI raises several critical questions for the future:

- ***Towards global AI governance?:*** The lack of global coordination on AI could lead to technological fragmentation, with each bloc (USA, EU, China) developing its own rules. International cooperation is essential to avoid regulatory chaos and ensure ethical and secure AI (Russell, 2021).
- ***The issue of digital sovereignty*** : The dominance of Big Tech (Google, Microsoft, OpenAI , NVIDIA) over AI infrastructure raises concerns about the independence of nations. Countries must invest in sovereign AI infrastructure to avoid dependence on foreign technologies.
- ***Ethics and social impact of AI*** : AI is already influencing critical decisions (health, justice, finance). It is becoming imperative to ensure the fairness and transparency of algorithms, avoiding algorithmic biases that can discriminate against certain population groups (Bender et al., 2021).
- ***Regulation of military AI and autonomous weapons:*** AI is now being integrated into autonomous military systems (drones, combat robots). The ethical question of using autonomous weapons without human control is a hot topic that could trigger a new type of geopolitical conflict (UNODA, 2023).

AI regulation is a complex challenge, requiring a balance between innovation and control. Europe, the United States, and China are taking different approaches, reflecting their respective visions of technology governance. However, the absence of a unified global regulatory framework could lead to fragmentation of the AI market, creating distinct technology blocs .

In the future, nations will need to cooperate to establish global standards while ensuring the safety, transparency, and ethics of AI. The race for supremacy in artificial intelligence will be won not only on technological grounds, but also on governance and legal frameworks. who will frame this revolution.

CONCLUSION

The First World War of AI is a silent but decisive technological war, in which supremacy in artificial intelligence is becoming a key factor in economic, military, and geopolitical power. This rivalry between nations and companies is not limited to a simple race for innovation, but extends to hardware architectures, learning models, cyber threats and defenses, and the regulations governing these advances.

One of the main issues in this war lies in the control of hardware infrastructure. The dominance of certain companies and nations over semiconductors and specialized computing units (GPUs, TPUs, ASICs) determines a country's ability to develop cutting-edge AI. Added to this is the algorithmic battle, where new deep learning models learning , including Transformers and LLMs , are redefining the standards of performance and efficiency of AI systems.

But this rapid advancement is not without risks. AI has become a digital weapon, capable of strengthening cybersecurity while facilitating autonomous and sophisticated attacks. Adversarial attacks , polymorphic malware, and AI-assisted phishing schemes exemplify this new form of cybercrime, rendering traditional defense systems obsolete in the face of constantly evolving threats.

In the face of these challenges, the issue of AI regulation and control is becoming paramount. *The European AI Act* , US policies based on sector-specific regulation, and China's centralized approach demonstrate the divergences in how each bloc attempts to control this revolution. However, the absence of *harmonized global governance* risks accentuating technological fragmentation and leading to an uncontrolled AI race.

The future of this technological war will therefore depend on the ability of nations to *reconcile innovation and security* , while ensuring the *transparency and ethics* of the systems deployed. While AI represents an unprecedented opportunity for progress, its use without an adequate framework could also lead to major abuses. Supremacy in artificial intelligence will not only be determined by the power of algorithms and infrastructures, but also by how these technologies are regulated and integrated into our societies.

This *First World War of AI* is therefore far from over, and its outcome will determine the technological balance of power in the 21st century.

REFERENCES

1. Works and monographs

1. Benedict, C., & Agrawal, A. (2021). *Machine Learning Systems: Designs, Concepts, and Applications for Engineers and Data Scientists.* CRC Press .
2. Goodfellow , I., Bengio , Y., & Courville , A. (2016). *Deep Learning.* MIT Press .
3. Hennessy, J.L., & Patterson, D.A. (2019). *Computer Architecture: A Quantitative Approach.* Morgan Kaufmann.

4. Russell, S. (2021). *Human Compatible: Artificial Intelligence and the Problem of Control.* Penguin Random House.
5. Saxe, J., & Sanders, K. (2017). *Malware Data Science: Attack Detection and Attribution.* No Starch Press .

2. Scientific articles and communications

1. Anderson, H.S., Woodbridge, J., & Filar , B. (2018). *DeepDGA : Adversarially -tuned domain generation and detection.* Proceedings of the 25th Network and Distributed System Security Symposium (NDSS).
2. Bender, E.M., Gebru , T., McMillan-Major, A., & Shmitchell , S. (2021). *On the dangers of stochastic parrots: Can language models be too big?* Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, 610–623.
3. Brown, T., Mann, B., Ryder, N., Subbiah , M., Kaplan, J., Dhariwal , P. , ... & Amodei , D. (2020). *Language models are few-shot learners.* Advances in Neural Information Processing Systems, 33, 1877-1901.
4. Carlini , N., & Wagner, D. (2017). *Towards evaluating the robustness of neural networks.* 2017 IEEE Symposium on Security and Privacy (SP), 39-57.
5. Doshi -Velez, F., & Kim, B. (2017). *Towards a rigorous science of interpretable machine learning.* arXiv preprint arXiv:1702.08608.
6. Dosovitskiy , A., Beyer, L., Kolesnikov , A., Weissenborn , D., Zhai , X., Unterthiner , T. , ... & Houlsby , N. (2021). *An image is worth 16x16 words: Transformers for image recognition at scale.* arXiv preprint arXiv:2010.11929.
7. Goodfellow , I., Shlens , J., & Szegedy , C. (2014). *Explaining and harnessing adversarial examples.* arXiv preprint arXiv:1412.6572.
8. Han, S., Pool, J., Tran, J., & Dally, W. (2015). *Learning both weights and connections for efficient neural networks.* Advances in Neural Information Processing Systems , 28.
9. Hinton, G., Vinyals , O., & Dean, J. (2015). *Distilling the knowledge in a neural network.* arXiv preprint arXiv:1503.02531.
10. Hodo, E., Bellekens , X., Hamilton, A., Dubouilh , PL, Iorkyase , E., Tachtatzis , C., & Atkinson, R. (2017). *Threat analysis of IoT networks using artificial neural network intrusion detection system.* 2017 International Symposium on Networks, Computers and Communications (ISNCC), 1-6.
11. Huang, L., Joseph, A.D., Nelson, B., Rubinstein, B.I.P., & Tygar , J.D. (2011). *Adversarial machine learning.* Proceedings of the 4th ACM Workshop on Artificial Intelligence and Security, 39-50.
12. Jacob, B., Kligys , S., Chen, B., Zhu, M., Tang, M., Howard, A. , ... & Adam, H. (2018). *Quantization and training of neural networks for efficient integer-arithmetic-only inference.* Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2704-2713.
13. Kingma , D.P., & Ba, J. (2014). *Adam: A method for stochastic optimization.* arXiv preprint arXiv:1412.6980.
14. Konečný , J., McMahan, HB, Yu, FX, Richtárik , P., Suresh, AT, & Bacon, D. (2016). *Federated learning: Strategies for improving communication efficiency.* arXiv preprint arXiv:1610.05492.
15. Kurakin , A., Goodfellow , I., & Bengio , S. (2017). *Adversarial examples in the physical world.* arXiv preprint arXiv:1607.02533.
16. LeCun , Y., Bengio , Y., & Hinton, G. (2015). *Deep learning.* Nature, 521(7553), 436-444. https://doi.org/10.1038/nature14539
17. Li, H., Ota, K., & Dong, M. (2018). *Learning IoT security mechanisms via a federated approach: A decentralized and collaborative strategy.* IEEE Communications Magazine, 56(10), 48-54.
18. Liu, Z., Lin, Y., Cao, Y., Hu, H., Wei, Y., Zhang, Z. , ... & Guo , B. (2021). *Swin transformer: Hierarchical vision transformer using shifted windows.* Proceedings of the IEEE/CVF International Conference on Computer Vision, 10012-10022.
19. Madry , A., Makelov , A., Schmidt, L., Tsipras, D., & Vladu , A. (2018). *Towards deep learning models resistant to adversarial attacks.* arXiv preprint arXiv:1706.06083.
20. Silver, D., Schrittwieser , J., Simonyan , K., Antonoglou , I., Huang, A., Guez , A. , ... & Hassabis, D. (2017). *Mastering the game of Go without human knowledge.* Nature, 550(7676), 354-359. https://doi.org/10.1038/nature24270
21. Vaswani , A., Shazeer , N., Parmar , N., Uszkoreit , J., Jones, L., Gomez, AN, ... & Polosukhin , I. (2017). *Attention is all you need.* Advances in Neural Information Processing Systems, 30.

3. Institutional documents and official reports

1. European Commission. (2023). *Artificial Intelligence Act: Proposal for a regulation laying down harmonized rules on artificial intelligence.*
2. National AI Initiative Act . (2021). *US National Artificial Intelligence Initiative Act of 2020.*
3. UNODA. (2023). *Lethal Autonomous Weapon Systems and International Law.* United Nations Office for Disarmament Affairs .
4. Xinhua. (2022). *China's AI Development Strategy and Regulations.* Xinhua News Agency.

4. Electronic sources

1. NVIDIA Corporation. (2023). *NVIDIA A100 Tensor Core GPU: Unleashing AI and HPC.* Retrieved from https://www.nvidia.com/en-us/data-center/a100/
2. TSMC. (2023). *TSMC Technology Roadmap: The Future of Semiconductor Manufacturing.* Retrieved from https://www.tsmc.com/english/home