ORYXLABS

RESEARCH

AL AIN

AI-ENABLED CYBERCAPABILITIES IN 2024, AND A LOOK BEYOND

CONTENTS

Foreword - An Early Vision 1

Introduction - AI and The CyberEye 2

A New Set of Capabilities 3

AI-Enabled Cyber Tools 4

AI, A Forge for Cyber 6

As Demanding as Powerful 7

The ACD Triangle 8

AI Ain - The Eye that Steers 10

References 11

FOREWORD
AN EARLY VISION

The quote is taken from a 2019 strategic article by Guyonneau & Le Dez, published in West Point's Cyber Defense Review, addressing the **impact of AI in the context of cyberwarfare** [1].

Five years in, and **accounts emerge from the operational level** that report the development of capabilities that the article could only hint at then [2].

Here we develop further the impact of AI in cyberwarfare with a focus on the capabilities it enables so far.

We then consider the **conditions under which these capabilities can be achieved**, identifying the strategic importance of a national cyber defense platform to deploy them.

Finally, we take a step back on the topic of AI and cyberwarfare, to **offer perspectives on the strategical and the organizational levels**, hence completing the proposed picture, and vision.

> “
>
> AI is the key to cyberspace’s intelligibility. Without it, digital warfare will endure; with it, it will thrive.
>
> ”

DR. RUDY GUYONNEAU

Now Director of Research, ORYXLABS

INTRODUCTION
AI AND THE CYBEREYE

In the realm of modern warfare, the cyber domain has emerged as **the fifth battlefield,** joining land, sea, air, and space.

However, unlike the traditional domains, **cyberspace lacks a physical presence**: an eye to observe activity, a body to orient, a will to decide and a hand to act.

By its capacity to "*unearth relations within the data that would have escaped the expert's attention*"[1], or to "*learn and process information in ways that human reason alone cannot*" [3, p228], **AI is the eye that processes the situation at the same pace as the domain evolves**, since both AI – the vessel – and cyber – the space - are machine's.

Reducing the mathematical complexity of cyberspace to a limited set of human-friendly indicators, **AI provides the situational awareness the cyberoperators require** to perform theirs missions efficiently.

Announced as **a forge for decisive cybercapabilities** back in 2019, AI has seen multiples tools being developed that have been recently reported by a US Army Cyber Operations Officer [2].

The vision is turning into a reality.

A NEW SET OF CAPABILITIES

New capabilities demonstrate how AI can transform cyberwarfare by improving the speed, accuracy, and effectiveness of operations.

AI-ENABLED CYBER TOOLS

ENHANCED THREAT DETECTION AND RESPONSE

» ANOMALY DETECTION

The analysis of vast amounts of network and endpoint data to identify unusual patterns and behaviors indicative of cyber threats, allowing for quicker detection and response.

» AUTOMATED INCIDENT RESPONSE

The automation of routine tasks in incident response, such as isolating compromised systems, initiating containment protocols, and deploying countermeasures.

SIMULATION AND TRAINING

» REALISTIC SCENARIO GENERATION

The creation of dynamic, realistic training scenarios that simulate actual cyber threats and adversarial tactics, providing practical experience for cyber defenders.

» ADAPTIVE TRAINING PROGRAMS

The tailoring of training programs based on individual or team performance, ensuring that the training is relevant and targeted to specific needs.

ADVANCED INTELLIGENCE GATHERING

» AUTOMATED DATA COLLECTION AND ANALYSIS

AI to rapidly collect, translate, and synthesize data from multiple sources, providing concise and relevant intelligence reports for decision-makers.

» THREAT INTELLIGENCE INTEGRATION

AI to integrate real-time threat intelligence into security operations, ensuring that defenses are updated with the latest information on emerging threats.

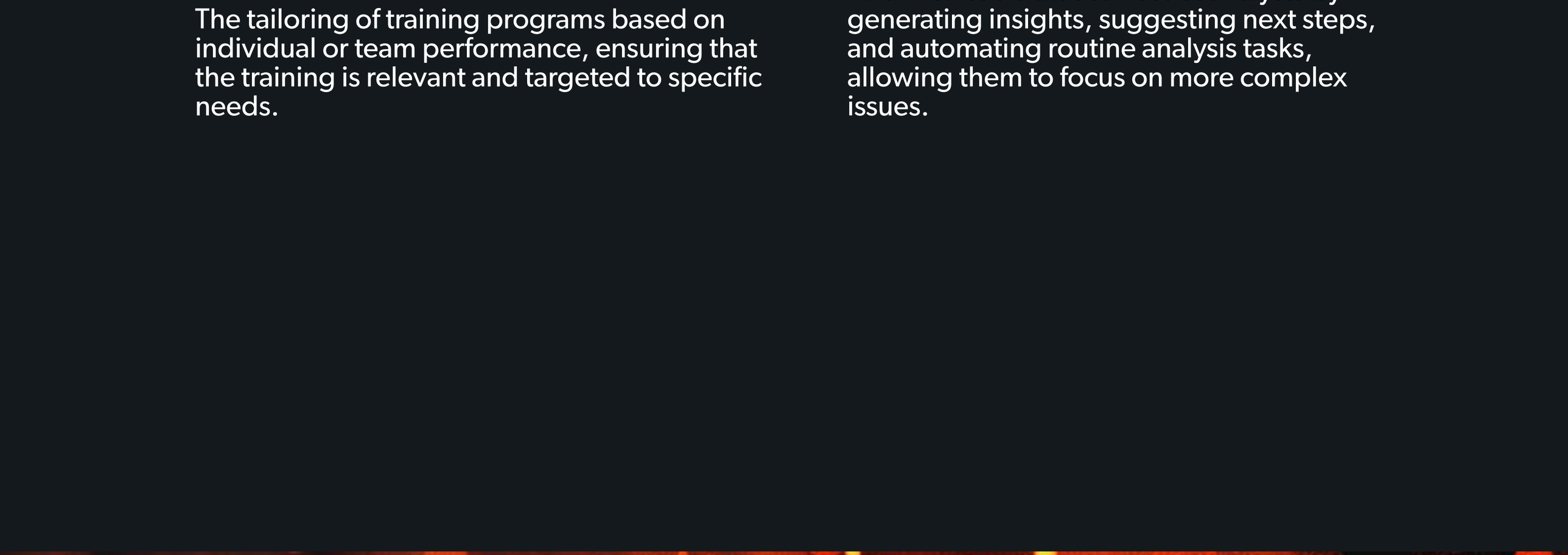
OPERATIONAL EFFICIENCY

» ACCELERATED ANALYSIS

AI to process and analyze large datasets much faster than humans, reducing the time required to identify and respond to threats.

» ANALYST SUPPORT TOOLS

AI-driven tools that can assist analysts by generating insights, suggesting next steps, and automating routine analysis tasks, allowing them to focus on more complex issues.



AI-ENABLED CYBER TOOLS

CYBER RANGE AUTOMATION

» ENVIRONMENT SETUP AND MANAGEMENT

Automating the creation and management of cyber ranges, setting up networks and systems that mirror real-world environments for training and testing.

» SYNTHETIC ACTORS

AI agents can simulate adversaries and other entities within cyber ranges, providing dynamic and interactive training experiences.

PREDICTIVE ANALYTICS AND FORECASTING

» PREDICTIVE THREAT MODELING

AI can predict potential cyber attacks by analyzing historical data and identifying patterns that suggest future threats.

» OPERATIONAL FORECASTING

AI can simulate the impact of different cyber defense strategies, helping organizations to plan and prepare more effectively.

MISCELLANEOUS

» ENHANCED DECISION-MAKING

AI can provide decision-makers with real-time, data-driven insights, enhancing their ability to make informed strategic and tactical decisions.

» PROACTIVE THREAT IDENTIFICATION

AI can continuously scan networks and systems for signs of potential threats, identifying and addressing vulnerabilities before they can be exploited.

RATIONALE

At the network level alone, cyberspace can be captured by endpoints and network sensors that produce billions of event per day, resulting in “data overload” for the operational personnel.

AI's journey in cybersecurity began with rule-based systems that could detect known threats. However, as cyber threats became more sophisticated and dynamic, these systems struggled to keep up.

Machine Learning (ML), the branch of AI responsible for GenAI, feeds on data with a neverending hunger. Its advent in cyberspace allows for more adaptive and responsive security measures. Today, with the rise of ML, capabilities are enabled that significantly enhance both defensive and offensive operations.

AI, A FORGE FOR CYBER

AI, as a technology, enables a new kind of tools, which display a particular kind of intelligence, not born of physical experience in the field, but of mathematical correlations observed at macroscales.

AS DEMANDING AS POWERFUL

Because it can **synthesize a vast amount of high-velocity data across multiple channels into a single mission-oriented indicator,** in real-time, AI gives cyberoperators the cybereye they were missing to then orient, decide and act.

For all its promises, and now its achievements, one should not overlook the **foundational principles** that explain the emergence of the current brand of AI; they also dictate its successful operational deployment.

These principles form the ACD triangle [1] of

- **Algorithms**, which implement the capacity for a machine to learn;
- **Computing power**, which allows a machine to meet the real-time conditions of its operating space, and
- **Data**, as the material for the machine to extract a solution from.

These pillars also represent a set of specific challenges a leader has to be aware of. Fortunately, they are also unique power opportunities.

GUIDELINES

When to apply AI then? When is it a differentiator? Some engineering principles light up the way here [4]:

- When the problem is **too complex** for coding using human logic;
- When the problem is **constantly changing**, resulting in costly software updates;
- When it is a **perceptive problem**, that is when it consists of multiple datasources one needs to make sense of, as a whole;
- When it is an **unstudied phenomenon**, where knowledge does not exist to guide actions.

And most importantly, when there are vast amounts of data.

These guidelines capture how well AI fits the challenges of cyberspace, as it remains a complex space, constantly evolving and opaque.

It is worth noting here that **cyberscience** is emerging as a scientific discipline, to bring methodology and rigor in taming cyberspace.

These guidelines are not cyber-specific and can be brought to any field where these conditions can be met. In the case of Electronic Warfare for example, AI can improve the identification, interception, and analysis of electronic signals to gather intelligence (SIGINT): AI will pick up weak signals the adversary might rely upon to bypass the attention of human operators.

THE ACD TRIANGLE

ADOPTION

UNDERSTANDING RATHER THAN EXPLAINING

Without adoption, a technology, no matter how impressive, is without value; **an AI system should be used and integrated seamlessly in an operator everyday's routine**, just like its sword, or its gun.

The **cognitive aspect of AI tools** is a challenge for adoption, as it disrupts our typical relation to machines; they now "talk" to us, seem to "understand" us. And we seem to do too towards machines, eventually mistaken them for fellow human beings. This relation will present itself as a pronounced dimension of cybercombat.

This cognitive capacity is merely **a consequence of the learning algorithms**, of the very architectures used in Machine Learning. It does so at the cost of explainability, whose loss is actually the manifestation of the new form of "intelligence", a machine's.

For them to adopt AI systems, **cyberoperators will need to understand them**, rather than explain them. As such, their training should involve a background in mathematics, ideally data science practice, and at least AI trainings, for them to **develop the flair necessary to act in the tempo of combat** alongside their teammate [1].

COSTS

THE PERSPECTIVE OF NEUROMORPHIC ENGINEERING

AI starts as a science.

At its current stage of development, AI is still massively expensive, not only to design and develop, but also to actually run, a fact that Microsoft brought up to light recently [5]. One would note it has been known for awhile but rather ignored so far [6].

Not that it matters in the end as long as it enables victory, but **the AI of today is heavy and demanding**, when the brain it is inspired from is not.

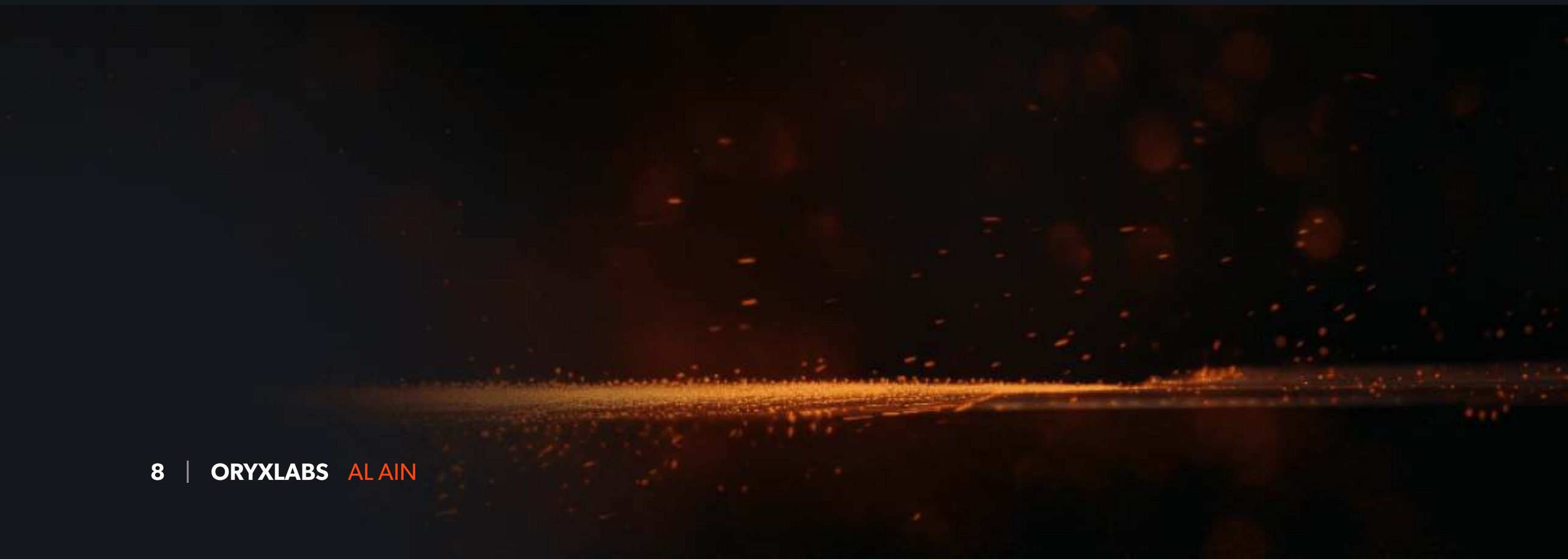
As a science, AI is constantly pushing forward, even though its pace might be slow. An evolution is coming, that might be overlooked: **Neuromorphic Engineering[1](NE), a brain-inspired approach to computing**, which optimizes energy consumption, at a comparable level of accuracy. If it hits as hard, while being lighter, which one would a combatant pick?

It is worth noting that the heavy computation of the current AI implementation implies reliance on cloud-based solutions. Two drawbacks stand out:

- **expansion of the attack surface**, synonymous to more exposure, and
- **increased latency** in the transmission of information between where the data matters and where it is processed.

Both aspects point towards edge computing approaches ("Edge AI"), of which NE is a part of, for an alternative to the fortress paradigm of cloud-based deployments.

[1] This was an evidence for Chinese research in 2019 [7].



THE ACD TRIANGLE

DATA

THE CASE FOR A NATIONAL CYBERDEFENSE PLATFORM

Data management is a a precondition to any successful AI implementations, military or not. Having data secured, high-fidelity and available determines the performance of AI systems.

It is then no surprise that Kissinger et al. place the **strategical stakes of "The Age of AI"** not so much around AI itself, but on "network platforms" [3]. This is the launching pad from where data is collected, refined, enriched and shared, resulting in networks effects that explain the success of the FAANGs[2] in the industrial world.

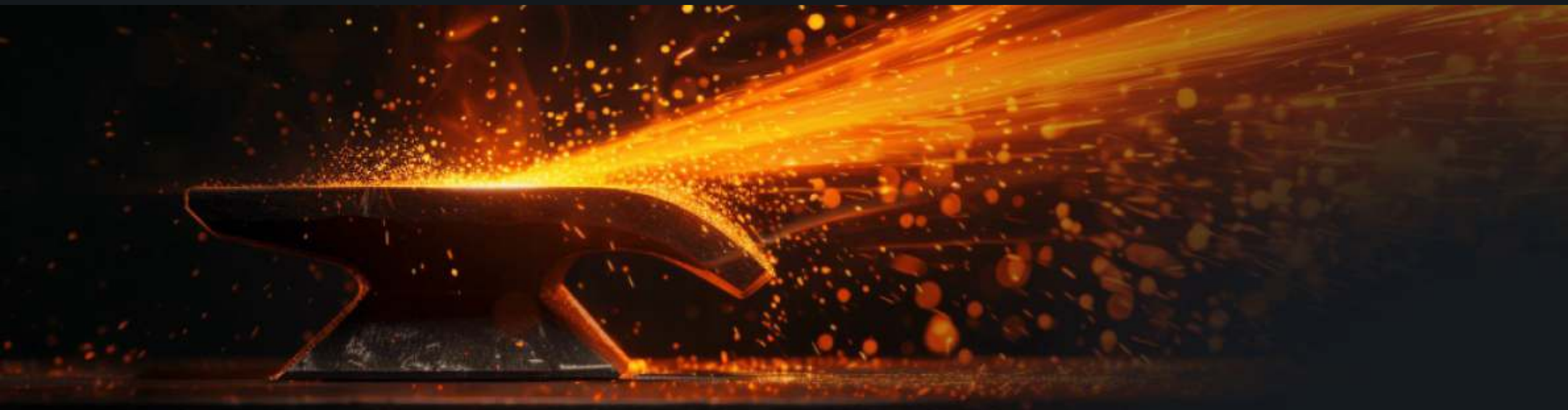
This is motivation for a national cyberdefense platform, to **capture and manage the cyberactivity related to the national space and its interests.**

Using Le Dez' distinction of cybercombat tactical phases [8], the platform would support

- the **identification of weaknesses** and enemy contacts [Security phase];
- the **prediction of its evolutions to enable maneuver** and regain initiative [Defense phase];
- so as to **stop the attack** and minimize damages [Attack phase].

Such a platform, **an anvil of sort**, would enable the deployment the cybercapabilities presented above, as well as the future ones to discover, design, and develop.

[2] Facebook, Amazon, Apple, Netflix, Google.



AL AIN
THE EYE THAT STEERS

AI addresses the challenges cyberspace poses to human cognition by operating at machine speed, building its own representation of the problems to solve. It produces cognitive tools, whose explainability is less important than the intelligence they can produce.

TACTICAL

The effect of AI on cyberwarfare is to **provide a situational awareness that meets the scale and complexity** of the fifth operating domain.

It also impacts the training of the personnel for them to eventually adopt a cyberteammate [1], a **machine with its own intelligence of the domain**, to assist in completing their mission.

ORGANIZATIONAL

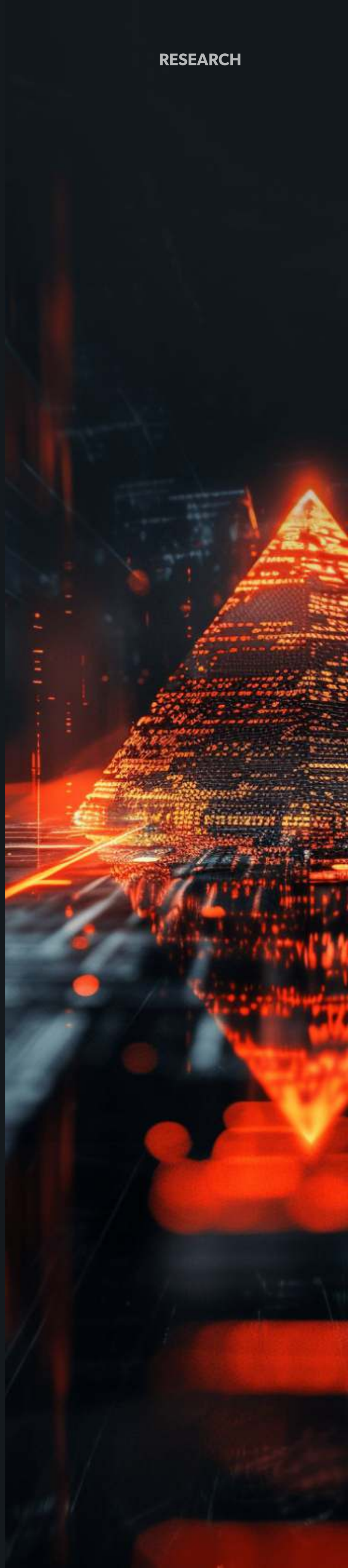
AI would also challenge the traditional, top-down approach to commandment, **amplifying the need for subsidiarity** recommended by leading researchers in cyberstrategy [8] [9].

In the everlasting sub-threshold cyberwar, AI would assist in strategically-aligned decision-making at the local level, by integrating the direction set by command, in the tempo of the battlefield. The **reversal of the hierarchical pyramid resulting from AI adoption in the cyberdomain** would imply adaptation by the layer traditionally in charge of combat management.

STRATEGIC

AI can support in the variety of tasks exposed to the data overload induced by the nature of the domain itself. More importantly, as we hope we showed throughout this state-of-the-art, under the right conditions, **AI can shift the advantage towards defense** [2], where it has been traditionally, and heavily, on the attack side.

It comes at great expense, and technological patience as well as scientific education, but it might very well be that, in the years to come, **a well-conceived AI proves itself to be the superiority factor in cyberoperations**.



REFERENCES

[1] Artificial Intelligence in Digital Warfare: Introducing the Concept of the Cyberteammate
Rudy Guyonneau and Arnaud Le Dez. Cyber Defense Review. 2019.

[2] Advantage Defense: Artificial Intelligence at the Tactical Cyber Edge
Zachary Szewczyk. Modern War Institute. 2024.

[3] The Age of AI: And Our Human Future
Henry A. Kissinger, Eric Schmidt, and Daniel Huttenlocher. John Murray Publishers, ISBN 978-1-529-37599-2. 2021.

[4] Machine Learning Engineering
Andriy Burkov. 978-1-999-57957-9. 2020.

[5] Our 2024 Environmental Sustainability Report
Brad Smith and Melanie Nakagawa, Microsoft. Self-published.

[6] Energy and Policy Considerations for Deep Learning in NLP
Emma Strubell, Ananya Ganesh, and Andrew McCallum. Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics. 2019.

[7] Towards artificial general intelligence with hybrid Tianjic chip architecture
Jing Pei et al. Nature (572). 2019.

[8] Tactique cyber - le combat numérique
Arnaud Le Dez. Economica, ISBN 978-2-71787-060-2. 2019.

[9] Guerilla 2.0: Guerres irrégulières dans le cyberespace
Bertrand Boyer. Ecole de Guerre, ISBN 978-2-35673-086-2. 2020.

ORYXLABS

21st Floor, Aldar HQ
Al Raha Beach
P.O. Box: 33289
Abu Dhabi, UAE

oryxlabs.com