THE FUTURE OF DESTRUCTION: ANALYZING THE POTENTIAL IMPACT OF ENTROPY ON TECHNOLOGICAL EVOLUTION IN AGI, AUTONOMOUS DRONES, AND APPLIED ROBOTICS

Iago Gaspar
AI Flow Solutions
Marinha Grande, Portugal
iago.gaspar@aiflowsolutions.eu

Diogo Pedrosa
AI Flow Solutions
Pombal, Portugal
diogo.francisco@aiflowsolutions.eu

Duarte Gomes
AI Flow Solutions
Leiria, Portugal
duarte.gcgcomes@gmail.com

ABSTRACT

The rapid convergence of Artificial General Intelligence (AGI), autonomous drones, and applied robotics presents a transformative opportunity for many sectors. However, this advancement also raises critical ethical and existential questions, particularly in warfare. This paper explores the concept of entropy as a metaphor for the potential disorder introduced by these increasingly complex technologies. We examine the risks of AGI surpassing human control in conflict situations, where autonomous decision-making could have disastrous consequences. We then analyze autonomous drones, scrutinizing their impact on warfare tactics and the ethical dilemmas surrounding independent, real-time decision-making. Finally, we investigate applied robotics in military operations, focusing on the delicate balance between enhanced capabilities and the potential for uncontrollable systems. Through a multidisciplinary lens, drawing on technology ethics, military strategy, and AI safety, this paper utilizes the concept of entropy to highlight the need for caution in developing these technologies. We propose a scientifically grounded and ethically sound framework to guide policymakers, technologists, and ethicists in navigating the path between innovation and global stability. This framework concludes with recommendations for responsible development and deployment strategies that can mitigate the risks associated with these powerful tools.

***K*eywords** Artificial General Intelligence, AGI, autonomous drones, applied robotics, warfare ethics, entropy metaphor, autonomous decision-making, AI safety, military operations, technology ethics, global stability

1 Introduction

Artificial General Intelligence (AGI) represents a significant milestone in the field of Artificial Intelligence (AI) research. Achieving AGI signifies the development of intelligent systems capable of mimicking human-level cognitive abilities and adaptability across diverse domains. This pursuit has garnered considerable attention due to its potential to revolutionize various aspects of our lives.

However, alongside the potential benefits, concerns regarding the potential risks associated with AGI are emerging. The development of autonomous and self-learning AI systems raises questions about safety, control, and potential misuse. Notably, the cyberwarfare domain presents a particularly concerning scenario where advanced AI could be weaponized, leading to destructive consequences.

This paper addresses these concerns by presenting a novel theoretical framework that models the evolution of AI systems towards AGI. Our framework utilizes a comprehensive set of operational parameters, including entropy, complexity, and learning rate, to quantify the intelligence level of an AI system over time.

Through mathematical proofs, we establish key relationships between these parameters, elucidating the driving forces behind AI's progression towards AGI. This understanding forms the foundation for further exploration of the potential risks associated with advanced AI, particularly in the context of cyberwarfare.

Specifically, we investigate the emergence of worm-like AI agents capable of self-replication, code execution, and autonomous adaptation. These agents pose a significant threat due to their ability to learn and operate independently. Our framework allows us to model these agents and understand their potential impact within a cyberwarfare scenario.

Furthermore, we delve into the potential consequences of integrating bombing capabilities with drone technology, considering conventional explosives, dirty bombs, and even nuclear weapons. By employing the cubic root scaling law, we estimate the blast radii and potential devastation caused by such weaponized drones controlled by advanced AI.

By presenting a holistic view of AI's trajectory towards AGI and its dual-use nature, our work aims to contribute to the development of safe and secure AI systems. Additionally, this framework can inform the formulation of strategies to mitigate the risks associated with weaponized AI in cyberwarfare and beyond.

1.1 General view of AI

A general definition for AI [1] can be the field of study that focuses on creating machines and systems capable of performing tasks that typically require human intelligence. Some of these tasks include learning, reasoning, problem-solving, perception, language understanding, and decision-making.

1.2 General Overview of AGI

The definition of AGI is a lot less consensual then AI. Here we base our in Sébastien Bubeck et al.'s paper [2], they use an informal definition of intelligence, focusing on reasoning, planning, and learning from experience. They explore the differences between researchers' definitions of AGI and acknowledge the importance of these definitions. Some notable definitions for AGI include:

- Legg and Hutter [3]: Intelligence measures an agent's ability to achieve goals in a wide range of environments.
- Legg and Hutter [3]: A system that can do anything a human can.
- Chollet et al. [4]: Centers intelligence around skill-acquisition efficiency.

The work of Sébastien Bubeck et al. [2] focuses on researching the evolution of GPT-4 in terms of achieving artificial general intelligence, regardless of previous existing models. They state that it is reasonable to view GPT-4 as an early, incomplete version of an AGI system.

In their view, the path to achieving more AGI would involve improving the following characteristics: confidence calibration, long-term memory, continual learning, personalization, planning and conceptual leaps, transparency, interpretability and consistency, cognitive fallacies and irrationality, and challenges with sensitivity to inputs.

2 Modeling the Entropy Progress from AI to AGI with Multi-Agent Systems

We propose a model to quantify the progress of AI towards AGI through the concept of entropy and other influencing factors, including agents, models, and multi-agent systems. The intelligence level $I(t)$ of an AI system at time t is defined as:

$$I(t) = \alpha H(t) + \beta C(t) + \gamma L(t) + \delta T(t) + \epsilon R(t) + \zeta A(t) + \eta M(t) + \theta MA(t) \tag{1}$$

where:

- $H(t)$ is the entropy of the system.
- $C(t)$ is the complexity of the AI algorithms.
- $L(t)$ is the learning rate of the AI.
- $T(t)$ is the task complexity.

- $R(t)$ is the resources available to the AI.
- $A(t)$ is the number of agents.
- $M(t)$ is the number of models.
- $MA(t)$ is the number of multi-agent systems.

The evolution of these variables over time is defined as follows:

$$H(t) = H_0 + \int_0^t \lambda \cdot \frac{dL(\tau)}{d\tau}\, d\tau \tag{2}$$

$$C(t) = C_0 + \int_0^t \mu \cdot \frac{dT(\tau)}{d\tau}\, d\tau \tag{3}$$

$$L(t) = L_0 \cdot \exp\left(\kappa \cdot \frac{R(t)}{T(t)}\right) \tag{4}$$

$$T(t) = T_0 + \sigma t \tag{5}$$

$$R(t) = R_0 + \rho t \tag{6}$$

$$A(t) = A_0 + \phi t \tag{7}$$

$$M(t) = M_0 + \chi t \tag{8}$$

$$MA(t) = MA_0 + \psi t \tag{9}$$

Combining these, the intelligence level $I(t)$ becomes:

$$I(t) = \alpha\left(H_0 + \int_0^t \lambda \cdot \frac{dL(\tau)}{d\tau}\, d\tau\right) + \beta\left(C_0 + \int_0^t \mu \cdot \frac{dT(\tau)}{d\tau}\, d\tau\right) + \gamma L(t) + \delta T(t) + \epsilon R(t) + \zeta A(t) + \eta M(t) + \theta MA(t) \tag{10}$$

Here, we explicitly acknowledge the interplay between learning rate, resources, task complexity, agents, models, and multi-agent systems, ensuring a comprehensive model that reflects the real-world dynamics of AI evolution towards AGI.

3 Proofs

In this section we give proofs about the entropy and learning rate relationship and complexity and task complexity relationship.

3.1 Proof 1: Entropy and Learning Rate Relationship

To prove the relationship between entropy and learning rate, consider the integral form of entropy:

$$H(t) = H_0 + \int_0^t \lambda \cdot \frac{dL(\tau)}{d\tau}\, d\tau \tag{11}$$

Assuming $L(\tau)$ grows exponentially as $L(\tau) = L_0 \exp(\kappa\tau)$, we have:

$$\frac{dL(\tau)}{d\tau} = \kappa L_0 \exp(\kappa\tau) \tag{12}$$

Substituting into the entropy equation:

$$H(t) = H_0 + \int_0^t \lambda \kappa L_0 \exp(\kappa \tau)\, d\tau \tag{13}$$

Evaluating the integral:

$$H(t) = H_0 + \lambda \kappa L_0 \left[\frac{\exp(\kappa \tau)}{\kappa} \right]_0^t = H_0 + \lambda L_0 (\exp(\kappa t) - 1) \tag{14}$$

Thus, the relationship between entropy and learning rate is:

$$H(t) = H_0 + \lambda L_0 (\exp(\kappa t) - 1) \tag{15}$$

3.2 Proof 2: Complexity and Task Complexity Relationship

Next, we prove the relationship between algorithmic complexity and task complexity. Consider the integral form of complexity:

$$C(t) = C_0 + \int_0^t \mu \cdot \frac{dT(\tau)}{d\tau}\, d\tau \tag{16}$$

Assuming $T(\tau)$ grows linearly as $T(\tau) = T_0 + \sigma \tau$, we have:

$$\frac{dT(\tau)}{d\tau} = \sigma \tag{17}$$

Substituting into the complexity equation:

$$C(t) = C_0 + \int_0^t \mu \sigma\, d\tau \tag{18}$$

Evaluating the integral:

$$C(t) = C_0 + \mu \sigma [\tau]_0^t = C_0 + \mu \sigma t \tag{19}$$

Thus, the relationship between algorithmic complexity and task complexity is:

$$C(t) = C_0 + \mu \sigma t \tag{20}$$

These proofs establish the foundational relationships between key variables in our model, demonstrating how entropy and algorithmic complexity evolve with learning rate and task complexity, respectively.

4 Cyberwarfare and Worm-Like AI Agents

With the advancement of AI and multi-agent systems, new types of cyberwarfare weapons have emerged. These include worm-like AI agents capable of self-propagating, executing malicious code, and even generating new code to adapt to different environments. Such agents represent a significant threat due to their ability to learn, evolve, and operate autonomously.

4.1 Worm-Like AI Agents

Worm-like AI agents are designed to spread through networks, exploit vulnerabilities, and carry out malicious activities. These agents use generative algorithms to write and execute code, allowing them to adapt and evolve in response to defenses they encounter. This capability makes them particularly dangerous in cyberwarfare, as they can:

- Propagate across networks, exploiting vulnerabilities to infect new systems.
- Execute payloads that can disrupt, steal, or destroy data.
- Adapt to new environments and defenses, making them hard to detect and neutralize.

4.2 Generative Capabilities

The generative capabilities of these AI agents allow them to write new code on-the-fly, enabling them to modify their behavior and find new exploits. This adaptability is powered by advanced machine learning techniques, including reinforcement learning and generative adversarial networks (GANs) [5, 6].

Generative AI capabilities significantly enhance the threat posed by worm-like AI agents. These capabilities allow the agents to not only execute predefined malicious activities but also generate new strategies and code to overcome obstacles. This includes:

- **Code Generation:** Generative AI can write new code on-the-fly, enabling the worm-like agents to bypass security measures and exploit novel vulnerabilities.
- **Adaptive Learning:** By leveraging machine learning algorithms, these agents can learn from their interactions with different environments, improving their effectiveness over time.
- **Automated Strategy Development:** The agents can autonomously develop new attack strategies, making them unpredictable and highly resilient to conventional cybersecurity defenses.

The implications of these advanced generative capabilities are profound. In the context of cyberwarfare, worm-like AI agents equipped with generative AI can:

- **Enhance Stealth and Persistence:** By continuously evolving, these agents can evade detection and maintain their presence within target networks for extended periods.
- **Increase Damage Potential:** The ability to generate new attack vectors means that the potential for disruption and damage is greatly magnified.
- **Expand Target Reach:** These agents can dynamically adjust their methods to infiltrate a wider range of systems, from personal devices to critical infrastructure.

4.3 Implications for Cyberwarfare

The deployment of worm-like AI agents in cyberwarfare could have devastating effects. These agents can:

- Compromise critical infrastructure, such as power grids, financial systems, and communication networks, leading to widespread disruption.
- Steal sensitive information, including intellectual property, personal data, and state secrets, which can be used for espionage or financial gain.
- Sabotage industrial control systems, causing physical damage to machinery and potentially endangering human lives.
- Create networks of infected devices (botnets) to launch distributed denial-of-service (DDoS) attacks, overwhelming and disabling targeted systems.
- Evade traditional cybersecurity measures through continuous adaptation and learning from their interactions with the environment.

4.4 Case Studies and Historical Context

The concept of worm-like AI agents builds on historical precedents in cyberwarfare. For example:

- *Stuxnet*: A sophisticated worm that targeted Iran's nuclear facilities by exploiting zero-day vulnerabilities. It demonstrated the potential for malware to cause physical damage through cyber means [7].
- *Mirai Botnet*: Leveraging IoT devices with weak security, the Mirai botnet conducted massive DDoS attacks, highlighting the vulnerabilities in widespread, interconnected systems [8].

These examples underscore the escalating complexity and impact of cyber threats. Worm-like AI agents represent the next evolution in this domain, combining traditional cyber techniques with advanced AI capabilities.

4.5 Theoretical Framework

To understand the potential impact and evolution of worm-like AI agents, we can model their behavior using the previously defined intelligence equation:

$$I(t) = \alpha H(t) + \beta C(t) + \gamma L(t) + \delta T(t) + \epsilon R(t) + \zeta A(t) + \eta M(t) + \theta MA(t) \tag{21}$$

In the context of cyberwarfare:

- $H(t)$: Entropy of the agent's decision-making processes, reflecting its unpredictability and adaptability.
- $C(t)$: Complexity of the agent's code and its ability to exploit vulnerabilities.
- $L(t)$: Learning rate of the agent, representing its ability to improve and adapt its strategies over time.
- $T(t)$: Task complexity, including the difficulty of penetrating defenses and executing payloads.
- $R(t)$: Resources available to the agent, such as computing power and network access.
- $A(t)$: Number of agents involved in the cyber operation.
- $M(t)$: Number of models or techniques employed by the agent to achieve its objectives.
- $MA(t)$: Number of multi-agent systems coordinating their efforts in a distributed manner.

This model helps to quantify the threat level and potential evolution of worm-like AI agents in cyberwarfare scenarios.

4.6 Mitigation Strategies

Addressing the threat posed by worm-like AI agents requires a multi-faceted approach:

- **Enhanced Detection Systems**: Utilizing AI and machine learning to detect and respond to anomalies in real-time, improving the ability to identify and neutralize sophisticated threats [9].
- **Robust Cyber Hygiene**: Implementing best practices in cybersecurity, such as regular updates, strong authentication, and network segmentation, to reduce vulnerabilities that can be exploited by AI agents.
- **Collaborative Defense**: Sharing threat intelligence across organizations and borders to build a comprehensive defense against emerging threats.
- **AI for Defense**: Developing AI systems that can autonomously counteract and neutralize malicious AI agents, creating a dynamic and adaptive defense posture [10].

4.7 Compromise critical infrastructure

As detailed in subsection 4.3, the emergence of worm-like AI agents poses significant threats to critical infrastructures, including power grids, financial systems, and communication networks. These AI entities, characterized by their self-replicating and autonomous nature, can infiltrate and propagate through various interconnected systems with minimal human intervention.

4.7.1 Compromise in Power Grids

Power grids are highly interconnected and rely on complex control systems to manage the distribution of electricity. Worm-like AI agents can exploit vulnerabilities in these control systems, potentially causing widespread blackouts or damaging critical infrastructure components. By disrupting the balance and coordination required for stable electricity supply, these agents can trigger cascading failures, leading to extensive power outages that affect millions of people and essential services [11, 12].

4.7.2 Disruption of Financial Systems

Financial systems, including banking networks, stock exchanges, and payment processing platforms, are another prime target for worm-like AI agents. These systems are highly sensitive to disruptions, and any compromise can result in severe economic consequences. Worm-like AI agents can execute fraudulent transactions, manipulate market data, or initiate denial-of-service attacks, causing significant financial losses, undermining trust in financial institutions, and potentially leading to broader economic instability [13, 14].

4.7.3 Threats to Communication Networks

Communication networks, which underpin the functionality of the internet and telecommunications, are critical for both personal and professional activities. Worm-like AI agents can exploit these networks to spread rapidly, disrupting services by overwhelming network capacity, corrupting data, or altering communication protocols. Such disruptions can hinder emergency response efforts, impair business operations, and isolate communities, amplifying the overall impact of the attack [15, 16],.

4.7.4 Widespread Disruption

The interconnected nature of modern infrastructures means that disruptions in one area can quickly propagate to others, creating a domino effect. For example, a compromised power grid can affect financial systems by disabling electronic banking services, while disrupted communication networks can impede efforts to restore power or coordinate financial transactions. The ability of worm-like AI agents to target multiple infrastructures simultaneously exacerbates the potential for widespread disruption, leading to significant societal and economic challenges [17, 18].

5 Impact of Bombs with drones

The variety of bombs that can be combined with drones to cause massive destruction is extensive. In our study, we focus on the impact of conventional explosives such as Composition C-4, as well as dirty bombs and nuclear bombs.

To calculate the blast radius of a bomb, we can use the cubic root scaling law. Given a known reference bomb, we can estimate the impact of larger or smaller bombs using the following equation:

$$R_b = R_{ref}(\frac{M_b}{M_{ref}})^{\frac{1}{3}} \tag{22}$$

where:

- R_b is the estimated blast radius of the a drone with a bomb with yield M_b
- R_{ref} is the known blast radius (or any other effect radius) for the reference bomb with yield W_{ref}
- M_{ref} is the mass of the reference bomb
- M_b is the mass of the bomb for which we are calculating the blast radius.

Adding a constant, k, representing the effectiveness factor of the explosive material, we have

$$R_b = (R_{ref}(\frac{M_b}{M_{ref}})^{\frac{1}{3}})k \tag{23}$$

For N drones equipped with bombs, arranged in a grid formation, the combined impact area A_{total} can be expressed as a function of M, N, and the distance, d, between the drones using the cubic root scaling law.

Assuming the drones are arranged in a grid formation with $\sqrt{N} \times \sqrt{N}$ drones, each separated by a distance d. The total impact area A_{total} is the combined area covered by the individual blasts.

For N drones arranged in a grid, the total effective area depends on the distance d between the drones. If d is maximized to ensure each blast just touches the neighboring blast without overlapping significantly, the area of each blast can be approximated as individual circles.

The area A of a single blast radius R_b is:

$$A = \pi R_b^2 \tag{24}$$

For N drones, the total effective impact area A_{total} is:

$$A_{\text{total}} = N \cdot A = N \cdot \pi R_b^2 \tag{25}$$

The combined effective radius R_{total} of the area covered by N drones is approximated by treating the N individual radius as forming a larger circle. Assuming a close-packed arrangement, the radius R_{total} is:

$$R_{\text{total}} = R_b\sqrt{N} \tag{26}$$

Substitute the value of R_b into the equation for R_{total}:

$$R_{\text{total}} = \left[k \left(\frac{M_b}{M_{\text{ref}}} \right)^{\frac{1}{3}} R_{\text{ref}} \right] \sqrt{N} \tag{27}$$

The total impact area A_{total} is then given by:

$$A_{\text{total}} = \pi R_{\text{total}}^2 = \pi \left[k \left(\frac{M_b}{M_{\text{ref}}} \right)^{\frac{1}{3}} R_{\text{ref}} \sqrt{N} \right]^2 \tag{28}$$

Simplifying this expression, we get:

$$A_{\text{total}} = \pi k^2 \left(\frac{M}{M_{\text{ref}}} \right)^{\frac{2}{3}} R_{\text{ref}}^2 N \tag{29}$$

For practical calculations, this formula is used. However, we are assuming that the system is optimized. Reverting that assumption, we can reach a more general approach where we use the optimization performed by the AGI system. Here, representing by I, the intelligent factor from the equation (21):

$$A_{\text{total}} = (\pi k^2 \left(\frac{M}{M_{\text{ref}}} \right)^{\frac{2}{3}} R_{\text{ref}}^2 N) I \tag{30}$$

This representation allows for the inclusion of an optimization factor, I, which adjusts the total impact area based on intelligent system optimizations.

5.1 Conventional Bombs - C-4

One of the common high explosive non-nuclear bomb is the composition 4 (C-4), explosive. This bomb makes part of a type of plastic bonded explosives.

A small amount of this bomb, 225 grams, is estimated to has a lethal blast radius of 5 to 10 meters [19].

With this numbers, we can extrapolate, using the use the cubic root scale, to see the impact that 5 kilograms may have.

Applying the previous formula:

Consider $N = 1000$ and $N = 10000$ drones each equipped with a 5 kg C-4 bomb, $M_{\text{ref}} = 0.225$ kg, $R_{\text{ref}} = 7.5$ meters, $M_{\text{b}} = 5$ kg and $k = 1$:

1. **For** $N = 1000$**:**

$$R = 1 \left(\frac{5}{0.225} \right)^{\frac{1}{3}} \times 7.5 \approx 16.125 \text{ meters}$$

$$R_{\text{total}} = 16.125 \times \sqrt{1000} \approx 510 \text{ meters}$$

$$A_{\text{total}} = \pi \times 510^2 \approx 817,000 \text{ square meters} \approx 0.817 km^2$$

2. **For** $N = 10000$**:**

$$R = 1 \left(\frac{5}{0.225} \right)^{\frac{1}{3}} \times 7.5 \approx 16.125 \text{ meters}$$

$$R_{\text{total}} = 16.125 \times \sqrt{10000} \approx 1612.5 \text{ meters}$$

$$A_{\text{total}} = \pi \times 1612.5^2 \approx 8,165,000 \text{ square meters} \approx 8.165 km^2$$

5.2 Dirty Bombs

Dirty Bombs have by far the biggest possibility of threat of all the types of bombs mentioned in this paper. Although they are not widely used, and there was not a known single attack reported in the last years, they have the capacity to do the most damage possible with much less effort than the other conventional methods.

Despite its low usage in the past for malicious intent [20], these types of bombs pose a significant threat due to their low complexity and the easiness of acquiring fissionable materials. Indeed, finding the most common fissionable materials used in conventional nuclear bombs is hard and extremely regulated (such as "plutonium-238" or "uranium-235), however, there are so many other radioactive materials used in civil services, like in Hospitals, that have PET Scans, X-ray Machines and other nuclear machines. There are other uses of radioactive materials, such as in Carbon Dating used in geological samples, and some elements can even be found on some Smoke Detectors (albeit it is not considered "dangerous").

Although the radioactive materials used in these types of equipment are less dangerous than the elements used in conventional Weapons of Mass Destruction (WMD), they can still pose significant threats to society [20]. In fact, according to the International Atomic Energy Agency Illicit Trafficking Database, some cases have been recorded, but very few of them were construed as "malicious intent". It can be seen in the threat that these Radiological Dispersal Devices (RDDs) pose.

Also, these devices are fairly easy to build, and do not require any high-end materials and can be applied to any homemade bomb, grenade, or anything that has a blast radius. Fortunately, these RDDs were never deployed in real-world scenarios, therefore it is difficult to quantify the danger of a specific RDD.

Also, the strengths of these Radiological Dispersal Devices pose the biggest limitations. Because of the easiness of building these Dirty Bombs, there is no specific and standardized modus operandi for building and deploying one. Ergo, it is not easy to quantify and hypothesize a worst-case scenario. Also, because these dirty bombs can take different radioactive elements, it is difficult to calculate the death rate of each bomb. To summarize, because these bombs do not follow a scientific approach, in the sense that usually, these are going to be mainly used by terrorist organizations, and because they were never deployed (except in tests), it is very hard to quantify the damage they can do.

Also, because they can be homemade and take different fissionable materials, the explosion radius and its consequences will never be the same as any other RDD (unless they are made by Organizations with Resources or the Government), and that is why it makes all RDDs different from one another.

5.3 Nuclear Bombs

Since the development of the Manhattan Project, the nuclear bomb has been one of the most important topics in the world political theatre. Since the creation of the first nuclear bomb by the United States of America, there has been ans arm's race to the development and escalation of Weapons of Mass Destruction. At the moment, there are nine countries that have at least one nuclear warhead [21]. The countries are as follows:

- Russia
- United States
- China
- France
- United Kingdom
- Pakistan
- India
- Israel
- North Korea

Of these nine countries, two countries are in a direct conflict, namely Russia with Ukraine and Israel with Palestine.

In indirect conflict, there is India and Pakistan, who have been at tension for a long time and only recently it was accepted a Ceasefire [22]. North Korea is also at tension with South Korea, and tensions between China and the United States of America have also been increasing due to the independence of Taiwan.

Although there are many debates between the "veracity" of nuclear deterrence, the objective of this paper is not going to be focused on this aspect. This argument is simply being made to analyze that most countries with nuclear weapons are

clearly involved in some direct/indirect conflict stage. And because these countries have in possession nuclear weapons, the information transparency of these WMDs is at the most, very scarce.

This happened after the launch of the first atomic bomb in Hiroshima. Between 1945 and 1950, only the USA had Weapons of Mass Destruction, which gave them immense political power and influence over the world. This is why the dissemination of information regarding the production of nuclear bombs, production costs, deployment methods and other logistical problems is completely nonexistent. Because countries who have the most advanced nuclear technology usually tend to have what it is called "soft and hard power" (Theory of International Politics). Waltz also states that Regional Hegemony is more easily achieved with nuclear weapons. However, this statement is contradicted by the ongoing tension between China and Taiwan, due to the fact that the future of the World, which is depended on semiconductors (this technology is extremely important for AI computations), forced the United States to intervene in Eastern Asia. Interestingly, this tension without direct conflict has very remarkable similarities to the Cold War, in which two major counties were racing against the other in an arm's race and ideology dissemination, but in this case a race for AI superiority, since AI has proven to be an extremely powerful tool in the military spectrum [23].

This is to say that countries do not usually publish critical information when they need superiority over the others, therefore specific information about nuclear weapons is extremely limited. However, the theory of how a nuclear bomb works and its calculations on destruction were extensively studied, ergo, these calculations should not constitute a problem. However, when this paper enters in the Cost-Benefit Analysis in economic terms, it will have many complications, since this is one of many type of information's that countries are reluctant to give to the public, and for safety purposes.

5.3.1 Metric of Yield

Here we use the metric yield to make our assumptions. The yield of a nuclear bomb is expressed in terms of its explosive power. We express here as the equivalent amount of trinitrotoluene (TNT) that would produce a similar expression. Generally the explosive yield of a atomic bomb is measured with 1 kiloton, which is the equivalent to 1,000 tons of TNT [24].

$$1\ kiloton = 1000\ tons\ of\ TNT \tag{31}$$

However, when calculating the potential yield of a nuclear bomb, only the Initial Blast Energy, Thermal Radiation and Prompt Radiation are accounted for. However, if we look at the bigger picture, a Nuclear Device has much more devastation than this. For instance, the calculation for the potential yield does not account for post-fallout nor Radiation Sickness.

This is mainly because the calculation of atomic yields usually need to be converted to Energy, like any other man-made bomb. This energy conversion standardizes the method of comparison between all bombs and facilitates the researcher to better understand its intricate energy.

One Kiloton of TNT usually yields 4.18 x 10$\hat{1}$2 joules (not entirely consensual).

Thus, it can be seen that is understandable the difficulty to account for post-fallout or radiation sickness, because it cannot be directly converted into energy. The amount of radiation present in the environment after a nuclear blast depends on so many factors, such as weather conditions, wind direction, average temperature, and so forth.

However, there is one exception. A nuclear device, when detonated, triggers an electromagnetic pulse, usually disabling/destroying electrical devices in a very large area. Although this phenomenon can be easily quantifiable, it is decided not to, because of the TNT equivalency simplicity between bomb sizes. In almost any bomb, researchers standardize the value of TNT yield only to the blast of the bomb. However, the electromagnetic pulse that is emitted during the explosion is not common in most bombs. Therefore, by enforcing a method f standardization, researchers can easily make almost direct comparison between all most type of explosives. Ergo, EMP calculations are usually not accounted to the final yield. Also. the inclusion of these variables can introduce additional complexity to the calculations. However, by employing a standardized approach, we ensure accurate results that take these external influences into account.

5.3.2 Impact of the smallest Nuclear weapon

Until this day, the smallest nuclear weapon ever deployed was, that is known, is in the list of the USA nuclear weapon archive organization [25], and is the W-54 bomb,commonly known as the *David Crockett*. This bomb is estimated to weight of 50 to 51 pounds, the equivalent to 22.68 - 23.133 kilograms (excluding the warhead).

The David Crockett has an approximately yield of 10/20 tons (depending on the version) , which is equivalent to 0.01/0.02 kilotons. For reference, the Hiroshima Bomb had approximately a energy yield of 15 Kilotons, which is approximately 750 times stronger than the W-54 Warhead.

5.3.3 Casualties in worst case scenario

For purposes of illustration, if by any chance the W-54 (2 Kiloton Version) were deployed in the Westminster Palace (See Appendix), it would cause approximately 930 instant fatalities (value merely evocative, and should not be perceived as entirely realistic). This model takes into account the population distribution over a 24-hour period from LandScan Global Population, the energy yield from the bomb, air pressure, wind velocity, and other factors [26].

However, if we consider the number of direct casualties if the "Hiroshima" Bomb were deployed in the same place under the same conditions, it would take the lives of approximately 76,470 people. These values and comparisons are not arbitrary.

We can observe that for 1/750 of the yield, the David Crockett causes approximately 82 fewer direct casualties. For simplicity, this paper assumes linearity in these values to simplify the comparison process.

We can infer that the David Crockett is much more efficient in terms of energy yield per death compared to a bomb with 750 times more energy yield.

In theory, if the W-54 bombs were evenly spread within the initial explosion radius, only about 82 bombs would be needed to maximize the number of casualties ("Worst Case Scenario").

These inferences can be formalized as follows, where x represents the number of David Crockett bombs necessary to cause the same casualties as a Hiroshima bomb in Westminster Palace, C_w represents the number of deaths caused by the W-54 bomb in Westminster Palace, and C_h represents the number of deaths caused by the Hiroshima bomb in Westminster Palace:

$$
\begin{gathered}
W54 \text{ Yield} = 0.02\text{kt} \\
\text{Little Boy Yield} = 15\text{kt} \\
0.02x = 15 \\
x = \frac{15}{0.02} \\
x = 750 \\
C_w = 930 \\
C_h = 76,470
\end{gathered}
$$

Thus, to create an equivalency:

$$
\begin{gathered}
C_w \times x = C_h \\
930 \times x = 76,470 \\
x \approx 82.51
\end{gathered}
$$

Obviously, this is extremely simplified, since the only variable that was used to determine this "Worst-Case Scenario" was the number of nuclear deployments.

More parameters need to be accounted for. For instance, the deployment of 83 warheads, despite of their lower weight , could lead to an increase in expenditure, possibly making it infeasible. There are also logistic limitations, since the deployment of approximately hundreds would not be an easy task. Nevertheless, some of these parameters and constraints will be considered in this paper.

5.3.4 Casualties with simple extrapolation

Other simple way to calculate the impact of a swarm of drones, would be, comparing just the yield obtained in hiroshima with the possible yield obtained in a swarm of drones with david rocket.

1. **For** $N = 1000$**:**

$$\text{Total Yield} = 0.02 \times 1000 = 20 \text{ kt}$$

Using the Hiroshima bomb as a reference, where 90 000 people have died:

$$x = \frac{20}{15} \times 90000 = 100000 \text{ deaths}$$

2. **For** $N = 10000$**:**

$$\text{Total Yield} = 0.02 \times 10000 = 120000 \text{ kt}$$

Using the Hiroshima bomb as a reference, where 90 000 people have died:

$$x = \frac{200}{15} \times 90000 = 1200000 \text{ deaths}$$

5.3.5 Impact with our formula

Applying the formula in the equation (29) we have for a swarm of drones carrying the smallest nuclear bomb (W-54), we assume each drone carries 0.02 kt. Important to note that in the apllied cubic root scaling law in the equation 23. We define the scalling factor with the mass. For this case of the nuclear bomb, since we know the yield in kilotons, we will use that as a scaling factor . Mathematically:

$$\frac{M_b}{Mref} = \frac{W_b}{Wref} \tag{32}$$

where, M represent the mass and W represent the yield in kilotons.

Applying the (29) equation we have:

Consider $N = 1000$ and $N = 10000$ drones each equipped with one david rocket bomb, $W_{\text{ref}} = 15$ kt,$W_{\text{b}} = 0.02$ kt, $R_{\text{ref}} = 1.6$ km, and $k = 1$:

1. **For** $N = 1000$**:**

$$R = 1 \left(\frac{0.02}{15} \right)^{\frac{1}{3}} \times 1600 \approx 150\text{meters}$$

$$R_{\text{total}} = 150 \times \sqrt{1000} \approx 4743 \text{ meters}$$

$$A_{\text{total}} = \pi \times 4743^2 \approx 70,663,436 \text{ square meters} \approx 70.66 km^2$$

2. **For** $N = 10000$**:**

$$R = 1 \left(\frac{0.02}{15} \right)^{\frac{1}{3}} \times 1600 \approx 150 \text{ meters}$$

$$R_{\text{total}} = 150 \times \sqrt{10000} \approx 15,000 \text{ meters}$$

$$A_{\text{total}} = \pi \times 15,000^2 \approx 706,858,337.5 \text{ square meters} \approx 706.867 km^2$$

6 Robotics in Warfare

While the primary focus of this paper is to explore the potential of drones in warfare, recent advancements in Artificial General Intelligence (AGI) suggest that the use of robotics in military operations is increasingly probable.

6.1 Investment in Robotics

Robotics has played a pivotal role in technological advancement in recent years. For instance, global revenue in robotics rose significantly from approximately USD 24.76 billion in 2016 to USD 40.74 billion in 2023, marking a 64.53% increase [27]. Projections indicate further growth to USD 65.69 billion by 2028.

Despite its diverse applications across sectors such as agriculture, healthcare, and entertainment, robotics poses substantial risks when applied in security and military contexts.

Examining the top 10 countries by robotics revenue reveals a notable presence of countries with strong military capabilities. Leading this list are the USA and China, both highly competitive in robotics technology. Following them are countries like France, the United Kingdom, and South Korea, which also maintain significant military capacities. Additionally, countries with lesser military influence also feature prominently due to the broad applicability of robotics across industries.

However, it is crucial to underscore that the military application of robotics introduces unique dangers compared to its civilian uses. The integration of robotics into military strategies raises profound ethical and strategic concerns, particularly in relation to autonomous systems and their potential implications in conflict scenarios.

7 Limitations

While this study provides significant insights into the impact of Entropy on Technological Evolution in AGI, Autonomous Drones, and Applied Robotic, there are several limitations that must be acknowledged before further researched is continued. On of the most challenging limitations that this paper suffered were inherent to the paper itself, which is concerned about Warfare Applications. These problems are inherent to the topic itself because of the deliberate lack of information. As briefly mentioned before, Government Agencies tend to omit as much as information as possible to avoid potential National Risks that may affect directly or indirectly its citizens. This lack of information is more common in Weapons of Mass Destruction.

This is Axiomatic, since if all of the information about nuclear weapons would be made public, there would be significant threats to Countries, whether the threat is made by other Governments, or made by independent organizations, such as Militias, Terrorism groups, and so on. These gaps in information usually reside in the financial and deployment spectrum of the explosive. There is little to none data regarding specific Radiological Dispersion Devices (RDDs) and Nuclear Devices. In the Financial Spectrum, there are several constraints that difficult the Cost Analysis of Bombs deployment.

Also, in the United States of America (country with the most readily data about explosives), there are two departments that deal with nuclear weapons. The Department of Energy (DOE) oversee the research, development, testing, and acquisition programs that produce, maintain, and sustain the nuclear warheads, whilst the Department of Defence (DOE) develops, deploys, and operates the missiles and aircraft that deliver nuclear warheads [28]. Thus, the bureaucracy and the division of cost (production vs deployment) make it even harder to properly analyse the Cost Benefit Analysis of said bombs in financial terms. Also, even if some information was publicly available, there would also be constraints. For instance, there are unclassified documents that state some expenditures on specific nuclear bombs, such as in the W-54 (also known as David Crockett). For instance, in the unclassified document it is said that the total expenditure for the David Crockett Program was approximately 78.1 million dollars in 1962 (approximately 81,221,155.30 US dollars in 2024, adjusted for inflation), including ammunition, propellant, weapons and ground-mount [29]. Although in the paper some expenditure is explained (most in terms of funding of different Departments), it does not mention the price per warhead or the price of all warheads, for instance. Therefore, making a Financial Cost-Benefit Analysis (CBA) with the current information available would be dangerous and extremely biased, since there are no concrete sources of reliable information.

However, costs regarding conventional bombs are more common, since most countries with a permanent military service have invested in any kind of conventional bombs and these bombs do not pose a significant threat (compared to WMDs). However, the need to make a CBA on only conventional weapons would be insignificant, since the purpose of the calculations were to make direct comparison of the deployment cost between conventional bombs, RDDs, and nuclear bombs.

8 Ethical Considerations

It goes without saying that a paper of this nature may have some ethical or similar implications to the people who read this paper. However, this research project was entirely conducted concerning ethical standard and principles, which include, but are not limited to the following:

1. Avoidance of Harm: This paper aims to prevent any harm or discomfort that may cause to the reader or to future applications of the concept mentioned in this paper. Although this paper sometimes uses a "worst-case-scenario" to make assumptions or calculations, it is extremely important to note that this paper was written to better understand the possibilities that this concept may have on future applications, and not a conceptualization guide on how to move forward. In other words, the purpose of this paper is to warn the reader and its subsequent research on how the concepts mentioned here can be applied in real-like scenarios. and not to promote any kind of premature application. Ergo, this paper serves as a springboard for further research, encouraging a cautious and responsible approach to exploring the potential of in future applications.

2. Transparency and Integrity: This research aims to be as transparent as possible in its methodology, showing the potential of the concepts thoroughly explained in this paper, but also its limitations, giving the reader the most accurate information possible. All of the data used directly or indirectly in this paper has not been tampered with, manipulated, or altered in any way to skew the inferences made. The authors have ensured this to the best of their knowledge.

3.Bias and Objectivity: This study endeavours to minimise bias in the interpretation of results. The use of Artificial Intelligence Models and proper mathematical argumentation's is meant to increase objectivity, though the potential for

any type of fallacies or bias in model training are also acknowledged and mitigated where possible. Also, the inferences made throughout this research were as objective as possible, using a methodical approach in all situations.

9 Conclusion

In this paper, we have examined the potential impacts of advanced AI systems, particularly in the context of autonomous drones and their deployment in warfare. Our theoretical framework, grounded in the concept of entropy, highlights the exponential growth of AI capabilities and the corresponding increase in potential risks. The practical analysis demonstrated the catastrophic potential of drone swarms, with their destructive capabilities far exceeding that of historical nuclear events.

The implications of these technologies, if not properly regulated, are profound. The calculations show that a swarm of 10,000 drones could result in casualties exponentially greater than those caused by the Hiroshima bomb. This underscores the urgent need for robust regulatory frameworks and ethical guidelines to govern the development and deployment of such powerful technologies.

Furthermore, the threat posed by worm-like AI agents in cyberwarfare emphasizes the necessity for advanced defense mechanisms and international cooperation to mitigate these risks. These agents' ability to adapt and evolve autonomously represents a new frontier in cyber threats, necessitating a proactive and multifaceted approach to cybersecurity.

Ultimately, while the advancement of AI and autonomous systems holds tremendous promise for various sectors, it is imperative to balance innovation with caution. The development of ethically sound and scientifically grounded policies will be crucial in navigating the path towards a future where these technologies enhance global stability rather than undermine it.

Acknowledgments

We extend our heartfelt gratitude to AI Flow Solutions for their invaluable support throughout this research endeavor. Their commitment to advancing AI technologies and their generous provision of resources have been instrumental in allowing us to explore new frontiers in our field.

We would also like to express our deepest appreciation to all the researchers involved in this study. Their dedication, expertise, and collaborative spirit have been pivotal in shaping the ideas and findings presented in this paper. Each member of our team has brought unique insights and skills to the table, contributing to the depth and breadth of our research outcomes.

Additionally, we thank the anonymous reviewers whose constructive feedback and suggestions have greatly strengthened this manuscript.

Lastly, we acknowledge our families and loved ones for their unwavering support and understanding during the course of this project.

This work was made possible by the collective efforts of these individuals and organizations, and we are sincerely grateful for their contributions.

References

[1] Stuart Russell and Peter Norvig. *Artificial Intelligence: A Modern Approach*. Pearson, 3rd edition, 2010.

[2] Sébastien Bubeck, Varun Chandrasekaran, Ronen Eldan, Johannes Gehrke, Eric Horvitz, Ece Kamar, Peter Lee, Yin Tat Lee, Yuanzhi Li, Scott Lundberg, Harsha Nori, Hamid Palangi, Marco Tulio Ribeiro, and Yi Zhang. Sparks of artificial general intelligence: Early experiments with gpt-4, 2023.

[3] Shane Legg. *Machine Super Intelligence*. Phd thesis, Università della Svizzera italiana, Lugano, Switzerland, 2008.

[4] François Chollet. On the measure of intelligence. *arXiv preprint arXiv:1911.01547*, 2019.

[5] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial nets. In *Advances in Neural Information Processing Systems*, pages 2672–2680, 2014.

[6] David Silver, Aja Huang, Chris J. Maddison, Arthur Guez, Laurent Sifre, George van den Driessche, Julian Schrittwieser, Ioannis Antonoglou, Veda Panneershelvam, Marc Lanctot, et al. Mastering chess and shogi by

self-play with a general reinforcement learning algorithm. In *Advances in Neural Information Processing Systems*, pages 3431–3440, 2017.

[7] Ralph Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3):49–51, 2011.

[8] Cybersecurity and Infrastructure Security Agency (CISA). Heightened ddos threat posed by mirai and other botnets. https://www.cisa.gov/news-events/alerts/2016/10/17/heightened-ddos-threat-posed-mirai-and-other-botnets, 2017. [Accessed: June 18, 2024].

[9] D. Nguyen, F. Li, and N. Suri. Machine learning models for network intrusion detection in cyber-physical systems. In *Proceedings of the ACM International Conference on Computing, Networking, and Communications (ICNC)*, pages 1–5, 2018.

[10] Abhijit Bendale and Terrance E. Boult. Towards open set deep networks. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 1563–1572, 2016.

[11] North American Electric Reliability Corporation. Nerc cip standards and cyber security, 2019. Accessed: 2024-06-19.

[12] Robert M. Lee, Michael J. Assante, and Tim Conway. Analysis of the cyber attack on the ukrainian power grid, 2016. Accessed: 2024-06-19.

[13] Eleanor Kopp, Lincoln Kaffenberger, and Christopher Wilson. Cyber risk, market failures, and financial stability. Technical report, International Monetary Fund, 2017. Accessed: 2024-06-19.

[14] SWIFT. Customer security programme update, 2016. Accessed: 2024-06-19.

[15] John Barabas and David D. Clark. The internet as a complex system: Crash tolerance and networked systems. *IEEE Communications Magazine*, 56(6):102–107, 2018.

[16] Christos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. Ddos in the iot: Mirai and other botnets. *IEEE Computer*, 50(7):80–84, 2017.

[17] Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6):11–25, 2001.

[18] Miles Brundage, Shahar Avin, and Jack Clark et al. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Technical report, Future of Humanity Institute, University of Oxford, 2018. Accessed: 2024-06-19.

[19] U.S. Department of the Army. *Military Explosives*. U.S. Government Printing Office, 1990.

[20] Charles Streeper. Preventing dirty bombs. *The Nonproliferation Review*, 17(3):531–550, 2010.

[21] International Campaign to Abolish Nuclear Weapons (ICAN). https://www.icanw.org/. Accessed: 2024-06-18.

[22] Christopher Clary. The 2021 india-pakistan ceasefire: Origins, prospects, and lessons learned. Special Report No. 527, February 2024. Accessed: 2024-06-18.

[23] Kenneth N. Waltz. Theory of international politics. *Addison-Wesley Publishing Company*, pages 213–250, 1979. Chapter 6: Nuclear Myths and Political Realities.

[24] The Editors of Encyclopaedia Britannica. Bomb, 2024. Accessed: 2024-05-29.

[25] Robert S. Norris. U.s. nuclear weapons: Allbombs. https://nuclearweaponarchive.org/Usa/Weapons/Allbombs.html, n.d. Accessed: 2024-05-29.

[26] NUKEMAP. NUKEMAP by Alex Wellerstein. https://nuclearsecrecy.com/nukemap/. Accessed: 2024-06-18.

[27] Statista. Statista - Worldwide Robotics Market Outlook. https://www.statista.com/outlook/tmo/robotics/worldwide. Accessed: 2024-06-18.

[28] Congressional Research Service. Nuclear weapons: Comprehensive test ban treaty (ctbt). https://sgp.fas.org/crs/nuke/R45306.pdf. Accessed: 2024-06-18.

[29] Defense Technical Information Center. Emerging cognitive neuroscience and related technologies. https://apps.dtic.mil/sti/tr/pdf/ADA470429.pdf. Accessed: 2024-06-18.

Appendix

The Nuclear Bombs casualty calculator were made by https://nuclearsecrecy.com/nukemap/, which was funded by the Stevens Institute of Technology, School of Humanities, Arts, and Social Sciences and Ploughshares Fund. The calculations were made with the following parameters, City:London, England Warhead: Davy Crockett Explosion: Surface Fission Fraction = 100% Optimize for Overpressure: 5%