DOI: 10.53477/1842-9904-25-28

THE ROLE OF ARTIFICIAL INTELLIGENCE IN NUCLEAR DETERRENCE. HISTORY, APPLICATIONS AND THE FUTURE STRATEGIC BALANCE

Mario MARINOV, PhD*

Artificial Intelligence is garnering an increasing interest for application within the complex and dynamic state of nuclear deterrence between major global powers. The latent implications of increased incorporation of fully or semi-autonomous functions into key sets of systems within nuclear deterrence capabilities hold the potential for both reinforcing and undermining strategic stability. The paper explores the role of the broad set of solutions falling under the auspices of the general and popularly adopted term of AI in the nuclear deterrence equilibrium with a baseline focus on the largest nuclear powers of the U.S.A., Russia, and China. The historical evolution of automation around the creation of effective deterrence during the Cold War is the first point of analysis in a process of historical deconstruction and extrapolation of key trends, historical understandings and the definition of vital layers of deterrence provision, which can be a subject of improvement through automation. Subsequently, the paper provides for the three general types of AI automation – rule-based AI systems, machine/deep learning and foundation models, and how each relates to specific elements or layers, such as early warning, tracking, response calculation, and targeting, as well as some of the associated challenges. Finally, the paper provides an analysis of the consequences for nuclear deterrence in the sense of probable areas of incorporation, a shifting centre of gravity in nuclear capabilities, and some prospective scenarios of AI integration in both offensive and defensive systems.

Keywords: *AI; nuclear deterrence; nuclear weapons; AI nuclear nexus; strategic balance; U.S.A.; Russia; China.*

---

* ***Mario MARINOV, PhD, is a Researcher within the "National Security" Department, University of Library Studies and Information Technologies, Sofia, Bulgaria, as well as an independent security and defense expert in nuclear weapons and deterrence. E-mail: m.marinov@unibit.bg***

"Let a sword of Damocles hang over every head,
and you will witness a miracle – all war will stop instantly"
Alfred Nobel

Introduction

Well into the third decade of the twenty-first century, "Artificial Intelligence" (AI) has perhaps become the defining buzzwords shaping nearly every level of society. From the lowest social organizational level concerning individual daily life and everyday enquiries to the larger and far more complex structures of the state and its operations, the word "AI" has come to dominate the discourse of current and future development. Within the sphere of nuclear deterrence, AI has been a variable expected with great trepidation for many decades – most often associated with artistic scenarios of the world's end at the hands of a rogue artificial intelligence unleashing a nuclear holocaust upon humanity either due to its own malevolent designs or due to human hubris and culpability. The popular mind is full of such images, "Skynet", "WORP" or "AM", to name but a few. However, the technological "holy grail" of AI had remained elusive for decades and the proverbial AI apocalypse also faded into the background.

Amidst the background of the rapidly changing global security environment characterized by both renewed adversarial relations in a bipolar or tripolar system of security relations between the United States of America, the Russian Federation and the People's Republic of China, and renewed dynamics in nuclear rearmament, the role and implications of the latest and significant new technological civilizational layer of AI has come to again be at the focal point of current and future security considerations.

The main subject of analysis in this paper is the strategic nuclear balance in the twenty-first century, with particular attention to how the object of examination is placed on the incorporation within the specific elements of nuclear deterrence and the broader nuclear balance of advanced autonomous and semi-autonomous data analyses, computation, modelling and machine thinking and learning methods. These technologies, often collectively, but somewhat erroneously, referred to as "Artificial Intelligence" or "AI", are central to understanding how possible changes can be expected within the state of nuclear deterrence between the major global nuclear powers of the United States of America (U.S.A.), the Russian Federation (Russia) and the People's Republic of China (China). Moreover, the question of the potential roles and scenarios of artificial intelligence within the elements that make up nuclear deterrence, including detection, tracking, target selection and guidance, will be explored. A broader extrapolation is also made in relation to possible future developments in both offensive and defensive strategic potential, as well as the implications of large-scale horizontal and vertical integration of AI within the broader strategic nuclear balance. To achieve this, the history and general understanding of automation as part of nuclear deterrence is examined, with the subsequent examination of different contemporary approaches and models of AI.

Within the field of scientific research, the topic of AI and nuclear deterrence has gained increasing attention for less than a decade, concurrent with both the ardent advances made in AI technology and the general state of renewed nuclear rearmament and deterioration of security relations between the major powers. Between 2018 and 2019, the first set of key reports were released into the potential impact of AI on nuclear deterrence – Michael C. Horowitz in "The Promise and Peril of Artificial Intelligence: Understanding the Impact on Strategic Stability and Nuclear Risk", provided the first contemporary systematization of AI and nuclear stability, with a focus on the duality of both stabilizing and destabilizing effects, as well as separate fields of AI implementation. Around the same time, Edward Geist and Andrew J. Lohn's RAND Corporation report, "How Might Artificial Intelligence Affect the Risk of Nuclear War?" (2018), brought forward the possible future escalation pathways under the influence of expanded AI capability up to the year 2040 from the results of a series of workshops; in the 2019 SIPRI publication "The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk", three articles by authors Vincent Boulanin, John Borrie, Page Stoutland and Petr Topychkanov present a comprehensive review of the historical evolution of automation in nuclear deterrence, the future of machine learning and autonomy in nuclear weapon systems and the potential future evolution of both the US and Russian nuclear arsenals. Concurrently, similar publications were produced elsewhere, such as the 2019 Russian International Affairs Council report "Artificial Intelligence and Nuclear Weapons" by Dmitriy Stefanovich, which puts an accent on optimization and resilience creation in the Russian nuclear forces, but also the risks of escalation and vulnerability. It is reasonable to assume, as is even pointed out in some of the aforementioned literature, that serious consideration, research and even prototyping began long before the publicly released research, and more so as a continuation of Cold War-era efforts at automation with the added enabler of early modern AI technologies.

Between 2022 and 2025, the amount of research produced significantly increased across all major actors. Scholarly scientific discussions focused on whether AI might reinforce or degrade nuclear deterrence, with a broader consensus emerging that while risks are probable, they remain largely manageable. Consensus appears also on the topic of retaining the critical approach of "human-in-the-loop" in any future reconfiguration of future nuclear strike potential with the integration of AI, which is also enforced by official statements of involved state actors. During this same period and with a higher degree of importance, certain divergences in national approaches can be observed – in U.S. and Western literature, AI is viewed as a capability enhancer to be intertwined within existing systemic layers in order to increase efficiency at key stages of deterrence. Furthermore, a major focus is placed on the coalescence of AI in the nuclear security field with AI capabilities in the other military fields, such as the conventional and cyber, into a common future security paradigm. Whereas in the Russian and Chinese approaches the term "informatization" (информатизация/信息化) of war/ or warfare has gained greater and greater traction, whereby the entirety of the concept of military capabilities, combined with other levers of power assertion (informational, political, economic, financial, demographic), are to be fully transformed into a wholly new structure of state power potential under the influence of technologies such as AI and where the integration of information networks and their operations will be key.

At present, the published efforts at AI integration into nuclear weapons systems showcase integration into the lower systemic levels of unit maintenance, logistics and administration management with a near-term goal of communication and technical support optimization. The Russian approach further takes into account the peculiarities of historical security concerns, such as the perceived threats of strategic missile defense and the vulnerabilities to a decapitation strike combined with conventional and other asymmetric methods. As such, full automation at certain systemic levels to ensure second-strike capability are viewed positively in Russian discourse. However, of note is the general realization that the capabilities of the Russian Federation are limited when compared to those of the U.S.A. and China, which already have a head start in AI technologies, and thus a primary focus is placed on finding solutions to breach existing gaps or to ensure the strategic balance through other means. In 2025, the terminology of the "AI-Nuclear Nexus" has appeared, based on the CNAS report by Jacob Stokes et. al. "Averting AI Armageddon: U.S.- China-Russia Rivalry at the Nexus of Nuclear Weapons and Artificial Intelligence" and has begun to see wider adoption in policy and research papers. As a cumulative and overarching term, the AI-nuclear nexus encompasses the convergence of artificial intelligence technologies with nuclear weapons systems, nuclear strategy, and the operational and strategic infrastructure that underpins nuclear deterrence. The term includes how AI may be integrated into functions such as nuclear command, control, communications, and intelligence (NC3), early warning, target verification, risk assessment, logistics, and decision-support. Further, the prospects of how AI might alter the larger strategic nuclear balance, compress decision timelines, increase ambiguity or false alarms and how the adoption of AI in conventional military systems could become entangled with nuclear risk are encompassed within.

This paper employs a qualitative, concept-driven methodology to investigate the evolving relationship between artificial intelligence and nuclear deterrence. It begins by outlining the foundational concepts of deterrence and situating them within their historical trajectory, with particular attention to prior phases of automation in nuclear command, control, and related subsystems. Next, the study surveys and classifies contemporary forms of AI according to their underlying methods and capabilities, producing a structured typology. Each AI type is correspondingly mapped onto specific segments of the larger deterrence system to evaluate potential points of integration and impact. On this basis, the study extrapolates how AI integration may alter deterrence dynamics by reshaping stability, survivability, and escalation thresholds. The analysis culminates in a set of forward-looking scenarios, including AI-enabled offensive advantages, the acquisition of an edge in missile defense capabilities via AI integration and the strengthening of deterrence through defensive reinforcement, as well as the destabilizing implications of a major AI capability gap. Throughout, the research relies on secondary sources drawn from strategic studies, historical case analyses, and policy-oriented reports from institutions such as RAND, SIPRI and the Valdai Club, as well as military publications and journals, such as the Russian "Military Thinking", ensuring a triangulation of conceptual, empirical, and policy perspectives.

Several considerations and limitations in the scope of the paper are necessary. When addressing the subject of nuclear weapons systems and the general topic of nuclear deterrence, it must be acknowledged that the sole utilization of public sources has the implicit condition of outdated information. As strategic nuclear power remains one of the primary tools of ensuring the survival of the state both research and actionable projects are likely to far outpace publicly available information. Consequently, published research should be viewed as affirmation of already existing trends and processes, which have taken place or are taking place now. The role of AI in nuclear deterrence should be viewed through the prism of a single continuing process of expanding the offensive and defensive nuclear potential of the state through automation of processes and subsystems, which has been ongoing since the Cold War and with AI being the next logical step. In terms of the examined scope of nuclear deterrence, the research is focused on the U.S.A., Russia, and China as the primary subject of interest and study due to the quantitative and qualitative characteristics of their nuclear arsenals, as well the underlying potential and intent to integrate AI within the foreseeable future. China is added to the historical and traditional strategic nuclear balance between the U.S.A. and Russia due to both the strives made in developing AI technology and the efforts placed in expanding its nuclear arsenal, which has significantly expanded both in its size and technological sophistication. Regarding the literature base, the paper draws primarily from sources in the English and Russian languages, as the nature of security-related processes within China, aside from the exponential language barrier, offer few publicly available insights. Finally, the paper examines the role of AI in nuclear deterrence chiefly within the context of the offensive and defensive nuclear balance, thus excluding the discourse on the risks that AI integration poses to nuclear deterrence, when considering both the nuclear and the conventional domains and their interplay with nuclear stability.

1. The Historical Context of Automation in Nuclear Deterrence

The integration of semi- or fully-automated solutions into the nuclear deterrence equation is not a novelty of the modern digital era, but a long historical process, which has in fact been a key facilitator of effective deterrence for decades, dating back to the Cold War. To better understand and thus analyse future trends of integration of AI methods, the historical considerations surrounding nuclear deterrence and automation of processes must be considered first.

At its core, "nuclear deterrence" refers to a condition of strategic balance between given nuclear powers, where the possession and credible threat of employing nuclear weapons, particularly strategic ones, prevents one side from initiating large-scale aggression due to the anticipated costs of retaliation outweighing the potential gains. A credible and effective state of deterrence is maintained through a number of factors, such as a survivable and attritable arsenal, providing an assured second-strike capability. Historically, effective deterrence has evolved to a state of strategic nuclear balance in the system of security relations between a set of nation states, encompassing key qualitative and quantitative characteristics of nuclear power.

At its core, a diverse and quantitatively sufficient strategic nuclear arsenal, comprising a nuclear triad of land, sea and air-based strategic nuclear assets, ensures a sufficient second-strike capability, thereby decreasing the possibility of a decapitation strike. The specific doctrinal characteristics of a nuclear triad encompassing launch platforms, be they hardened silos, dispersed mobile launchers, missile-carrying submarines in protected bastions and in undisclosed locations, or strategic bombers in dispersed airfields and constant patrols, provide the conditions for an effective deterrence. Similarly, the technological sophistication of nuclear warhead carriers themselves – intercontinental ballistic missiles (ICBMs), (submarine-launched ballistic missiles (SLBMs), and air-launched cruise missiles (ACMs), through the use of multiple independent warheads, decoys, penetration aids, active manoeuvring capabilities, or electronic countermeasures, further ensures a sufficient retaliatory response. In quantitative terms, the strategic strike potential of the nuclear triad must be available in sufficient numbers, dispersed and protected, to ensure that even if any given launch platform or a group of platforms is disabled, a credible retaliatory capability remains intact, to retaliate and incur unacceptable losses to the adversary. Whilst the nuclear triad captures in equal parts public attention, strategic discourse and past treaty regulations, the effectiveness of nuclear deterrence encompasses a broader set of systemic functions and further depends on sophisticated supporting systems that enable detection, tracking, communication, and targeting capabilities. These systems form the complex architecture of Nuclear Command, Control, and Communications (NC3), which serves as the critical link between launch authority and deployed nuclear forces. The NC3 system performs several fundamental functions: detection, tracking, warning and attack characterization in addition to the combat use of nuclear weapons, including the facilitation of decision-making procedures, preparation of launch orders, and their transmission to the implementation level (Yarynich 2003, 17, US Department of Defense 2020). Throughout the Cold War and the technological evolution of nuclear arsenals, significant efforts were concentrated on enhancing the NC3 process, encompassing both the ability to detect an incoming attack and launch a retaliatory strike, as well as the ability to coordinate defensive measures. From an early stage, these advancements reached towards semi-automated solutions.

1.1. The First Large-Scale Achievement in Automation. The Semi-Automatic Ground Environment (SAGE) System

The Semi-Automatic Ground Environment (SAGE) system, developed during the 1950s and deployed in 1963, represented the first large-scale integration of automation and computing technology into strategic defense operations and nuclear deterrence. SAGE emerged from the chief nuclear attack vector of the time, namely strategic bombers, and both the valid and invalid concerns regarding the Soviet Union's potential for bomber-based nuclear strikes (Boulanin, et al. 2019, 44). The exposure of U.S. bombers stationed on strategic airbases, and the inadequacies of existing air defense systems to handle interception on the strategic level, specifically high-speed interception, low-altitude radar coverage, and complex air tracking, led to the demand for a vast undertaking to improve U.S. defense capabilities. The system integrated a network of hundreds of radar stations across North America, with twenty-four direction centers and three combat centers with centralized data processing facilities powered by the IBM AN/FSQ-7 computer systems – among the largest discrete component computers ever constructed. (MITRE Partnership Network n.d.).

SAGE's operational concept pioneered many principles that would later become standard in subsequent nuclear automation systems. The system automatically processed raw radar data to develop target tracking solutions, calculated intercept solutions, and transmitted engagement commands to defense sites via teleprinter. Human operators retained ultimate authority over engagement decisions, however they operated within an automated framework that dramatically enhanced their situational awareness and overall response capabilities (Tobey 1959). By the time the system matured in the early 1960s, with the corresponding ground infrastructure and computing capacities becoming available, the strategic bomber had given way to the intercontinental ballistic missile (ICBM) and later on also to the submarine-based ballistic missile (SLBM), thus rendering an extensive air tracking and direction system increasingly redundant (Boulanin, et al. 2019, 44). Regardless, the principles and capability enablers of an automated system would be applied in the subsequent evolution of NC3 during the missile era.

1.2. Automation in NC3. The Strategic Automated Command and Control System (SACCS)

The introduction of ICBMs and SLBMs created the complex conditions of greatly decreased warning times in case of nuclear escalation. Moreover, the lack of effective countermeasures at the time, ensured that any massive attack would result in equally devastating consequences in terms of remaining retaliatory response instruments. Thus, both U.S. and Soviet nuclear doctrines adjusted in the 1960s to include the shortened decision-making timelines of potential nuclear escalation. The emergence of launch-on-warning strategies in both the United States and the Soviet Union highlighted the necessity of automated and semi-automated systems to strengthen early-warning reliability, ensuring decision makers received information promptly and gained crucial time to authorize the launch of nuclear countermeasures (Boulanin, et al. 2019, 44).

Within the evolution of U.S. nuclear deterrence capabilities, a critical stage was the implementation of automation on a system-wide level in NC3. The overarching system of the Strategic Automated Command and Control System (SACCS) achieved operational capability on January 1, 1968. SACCS provided the primary network for transmitting Emergency Action Messages (EAMs) between the National Command Authority and strategic nuclear forces, which included all elements of the nuclear triad – ICBMs, SSBNs and nuclear bombers. The system managed critical secure communications for force status monitoring, intelligence distribution, strategic planning, and post-strike damage assessment functions essential to nuclear operations. Unlike SAGE's strategic air defense mission, SACCS operated at the apex of nuclear decision-making, serving as a processing and distribution node for sensitive information and the coordination of nuclear response options. The system's hierarchical processor architecture and secure communication protocols established templates for subsequent nuclear command systems (Federation of Atomic Scientists 1999, Schance 1998).

SACCS innovations in automated message processing and secure communications became foundational elements of modern NC3 systems. The system's ability to provide full-duplex, secure data communications across dozens of active nodes illustrated the scale and complexity of nuclear command networks. Furthermore, the introduction of SACCS reinforced deterrence at a crucial stage of the Cold War when strategic offensive nuclear arsenals were vastly expanding and the offensive potential was greatly improved through diverse technical solutions such as enhanced targeting, multiple warheads and decoy deployment.

1.3. Fail-Deadly. Automation of Retaliation and the Soviet "Dead Hand" System

At the pinnacle of Cold War-era developments lies the Soviet fail-deadly system, often referred to as "Dead Hand" or "Perimetr", although the actual designation is unknown and whether "Perimetr" is the designation of a subcomponent or the entire system (Boulanin, et al. 2019). Developed during the 1970s and reported to have achieved operational status around 1985, Perimetr encompasses a vertically multilayered system within Soviet and later Russian offensive nuclear strike capabilities. The existence and purpose of Perimetr have been publicly declared (Boulanin, et al. 2019, 72), namely to ensure a retaliatory capability in conditions of degraded command and control, including those arising from a decapitation strike on the political and military leadership. The system encompasses an array of dispersed environmental sensors – seismic, radiation, light and pressure; connectivity checks – whether command and control function remains with designated political and military decision-making centres; as well as inputs from the larger space and land-based detection and tracking infrastructure (Horowitz, Scharre and Velez-Green 2019, 17). The purpose of the sensory layer of the system is to detect if an anomaly has occurred, i.e. a nuclear attack, whether occurring in real time or having already taken place, and to superimpose it with the eventuality and conditionalities of loss of command links and lack of corresponding retaliatory strike commands (Schwartz and Horowitz 2025, 2). Furthermore, the system features an automated signal subsystem, whose primary objective is to distribute launch commands to existing or remaining offensive nuclear assets, thereby enabling a retaliatory second-strike capability. An element of the signal system, namely the contemporary Sirena-M missile system, is publicly acknowledged and has the objective to conduct a launch over Russian territory when activated and transmitting launch orders to nuclear assets whilst in flight. There are numerous ambiguities and uncertainties in relation to Perimetr, particularly concerning its precise level of automation, system architecture and operational modes. A logical supposition is that Perimetr has several modes of operation, which can be activated depending on the general state of the security situation, which range in the level of automation of processes and the degree of human control – from a purely sensory network, which provides additional input to the traditional human-centric chain of retaliatory escalation to a semi-autonomous or fully autonomous detection, tracking, targeting and launch system, which can theoretically bypass different levels of higher and lower commands, if the programmed conditions are met. Considering the numerous instances of automated system failures throughout the Cold War, the introduction of Perimetr at a time of extreme tension preconditions the existence of either a very robust automated system of checks, or a final "human-in-the-loop" decision making mechanism. Overall, the standout feature of the system is apparent, to ensure second-strike capability under conditions of extreme degradation through a reliance of numerous robust, diverse and dispersed component subsystems, whose information input feeds through numerous verification pathways into a final automated launch solution. Thus, effective nuclear deterrence is achieved through an insurmountable obstacle to any type of first-strike by ensuring that the baseline conditions (loss of leadership combined with multiple sensory confirmations of an attack) would lead to automatic retaliation. Conversely, the interpretation and claim can also be placed forward that the heightened tensions of the 1980s and a perceived capability gap, created the conditions where one side would pursue the creation of a system, whose overreliance on automation could critically endanger deterrence in the case of a technical malfunction or as a result coerce an adversary to pre-empt the system's completion. Notwithstanding the peculiarities of historical security debates between the U.S.A. and Russia, Perimetr has never publicly entered the realm of discussion and treaty regulation.

For effectiveness, the vastness and complexity of the numerous subsystemic components encompassing and pertaining to nuclear deterrence require the introduction of technical solutions, which logically raised questions regarding varying degrees of automation. Overall, automation of processes during the Cold War was vital to achieving effective deterrence, which, in large part, has relied on and continues to rely on effective detection and early warning, as well as resilient NC3 capabilities. The introduction of automated solutions reinforced the belief that a surprise nuclear first strike could not be effectively achieved and, as in the case of the Dead Hand/Perimetr system, that retaliatory options could remain functional even in case of a decapitation strike. However, the centralization of information streams and processing into singular command and control systems with a large degree of automation predisposed risks and failures, which gave rise to several false-alarm incidents, such as in 1979 and 1980 in the U.S. with NORAD providing false alerts of an imminent attack, and the 1983 incident in the Soviet early-warning system, which similarly provided a false output of incoming U.S. missiles (Boulanin, et al. 2019, 46). It should be noted, however, that such incidents are often historically portrayed out of their original proportions, often to underline the theme of danger stemming from nuclear weapons and the integration of automated systems. In reality, by the time of the listed incidents - and throughout the entirety of the processes of system automation during the Cold War - a critical understanding was reached by both sides for the necessity of "human-in-the-loop" checks and controls, implemented not only at a single level but across numerous hierarchical levels within NC3. This understanding, underlined by some of the technical faults encountered in automated systems, remains in force to this day. Throughout the Cold War, more expansive levels of automation could potentially have been reached or sought after within several systems. One example is the early Cold War concepts for autonomous intercontinental bombers and cruise missiles, such as the U.S. SLAM and Soviet Burya projects, which could have required on-board fully automated processes (Geist 2023, 70). Another is the U.S. missile defense project Star Wars, which, due to its scale, complexity and technical challenges associated with combined ground- and space-based missile targeting and interception would also have required expansive autonomous modes for rapidly detecting, targeting and neutralizing ballistic missiles in quick succession and in a very limited timeframe.

In the contemporary era, the evolution of different AI-thinking approaches and their translation into a specific set of AI models possesses a vastly expanded transformative potential for the different elements of nuclear deterrence – either through incorporation into known subsystems encompassing NC3 or through enablement of novel capabilities in intelligence, surveillance, and reconnaissance (ISR). Problems encountered throughout the Cold War and later, which were insurmountable due to the level of processing power required and the complexity of processes could now be easily resolvable and could become pathways to a fundamentally altered landscape of nuclear deterrence.

2. Advances in Artificial Intelligence System Types and Models

Historically, automation provided solutions and improvements for key processes related to nuclear deterrence; however, past systems relied on simplified solutions limited by processing and computing power, providing only limited output to human operators. Revolutionary developments in digital technologies have brought about the prospects of significant changes in a variety of systems, ranging from baseline improvements to existing systems, such as early warning and tracking, to entirely new capabilities in detection, targeting, and simulation. The advances made in modern AI technologies and their further implementation in the nuclear deterrence equation depends on the core understanding and differentiation of the capabilities they afford, which can be subdivided into the different AI approaches, based on the technical methods used to input and process information and the quality of outputs, as well as the different AI models, which are built upon these approaches, and which encompass larger capabilities pertaining to the range of possible functions and quality of outputs.

2.1. AI Approaches

Artificial intelligence (AI) is often used to describe a wide variety of computational methods and approaches designed to enable machine-based systems to carry out tasks that would otherwise be assigned to humans. Such tasks include pattern recognition, natural language processing, environmental perception through computer vision, learning from prior experience, reasoning, and taking action. AI systems function in completing set tasks by inferring output from the received inputs - these outputs can be predictions, generated content, recommendations, or decisions. AI systems are generally developed through rule-based approaches and machine learning, includeing deep learning (Chernavskikh 2024, 2). These approaches give rise to several model types, most notably classification models, analytic and predictive models, and generative AI models (Stokes, et al. 2025, 2). Each AI approach and AI model offers certain capability enablers in the field of nuclear deterrence, and it is the often-accepted method of discussion in policy and research papers of expected transformative processes to occur in the future.

A **rule-based AI system** is an artificial intelligence approach in which decision-making or inference is governed by a set of explicitly codified rules, most often a form of "if *x* input or condition is met", "then provide *y* output". The system relies on a knowledge base of information and rules in addition to an inference engine to evaluate conditions and triggers for actions. It does not learn from data in the sense of updating rules automatically (though rules can be modified by human input), and it is usually deterministic – for a given input, if a rule's conditions are met, the outcome is fixed by the rule (Deepgram 2025, Science Direct n.d.). Rule-based AI is the longest-standing approach in AI due to its simplicity and has been a part of NC3 for decades, with Cold War systems such as SACCS and Perimetr being such types of "AI". In the current era, numerous elements of nuclear deterrence incorporate rule-based AI to provide outputs. For instance, missile early-warning systems utilize rule-based AI to detect ballistic missile launches and track their trajectories through ground- and space-based sensors. Beyond early detection, rule-based AI also plays a role in automated, secure communications, ensuring the rapid and reliable transmission of launch directives, emergency action messages in the event of a nuclear strike or retargeting commands inflight (Horowitz, Scharre and Velez-Green 2019, 15). In addition, rule-based AI applications extend to supporting fast and precise missile targeting, as well as improving missile guidance systems, thereby enhancing both the responsiveness and effectiveness of nuclear command and control (Chernavskikh 2024, 2, Horowitz, Scharre and Velez-Green 2019). Rule-based AI systems provide for predictable and consistent functionality, but suffer in terms of the limits of the core databases provided and the set rules, which would require constant updating by human operators. In the conditions of nuclear deterrence, rule-based AI is a core functionality in several layers, chiefly in detection and early warning, but also in communication, with its inherent redundancy in checks providing for greatly decreased chances of false-positives and misinterpretation of information (Protasov, Shirmanov and Radomanov 2023).

An improvement over rule-based AI, **Machine Learning (ML)** approaches, as well as expanded **Deep Learning (DL)**, provide for expanded potential capabilities. Machine learning refers to methods that enable computers to improve performance on tasks through experience, without being explicitly programmed for each outcome (Mitchell 1997, 2). ML systems include the iterative application of mathematical algorithms to datasets in order to find statistical patterns and reach required outputs. The statistical patterns, once created, form the fundamental basis of the ML system, which can then be applied in analyzing new data and providing output through inference (Chernavskikh 2024, 3).

Within the broader field of ML, deep learning represents a subset of techniques that employ multilayered neural networks to acquire hierarchical data representations and abstractions (LeCun, Bengio and Hinton 2015, 436–444, Goodfellow, Bengio and Courville 2016, 2). These architectures allow systems to perform highly complex tasks faster and can capture more intricate statistical relationships, such as computer vision, natural language processing, signal recognition, and data fusion (Chernavskikh 2024, 3). ML and DL are relatively new technologies, even though conceptually present even during the Cold War. The advances offered are substantial, specifically in the several layers of nuclear deterrence connected with processing vast amounts of sensory data and the construction of discernible patterns within – recognition and classification of objects based on a diverse set of input data, such as radar, visual and infrared feeds, which can allow for the prompt classification of objects such as mobile launchers or missiles in-flight and differentiation between warheads and decoys. To an even greater extent, the differentiation and classification of objects based on sensory data, such as acoustic or electromagnetic signatures, offers the ability to provide pinpointing of nuclear systems such as SSBNs on a limited subset of data (Boulanin, et al. 2019).

2.2. AI Models

Rule-based, machine learning, and deep learning approaches in AI systems represent successive stages in the application of artificial intelligence into specific models, each with implications for nuclear deterrence. Rule-based systems, with their rigidly encoded logic, underpin earlier applications such as missile early-warning systems and secure transmission of launch orders. ML, by contrast, *enables analytic and predictive models* that can learn from both established databases and real-time data inputs, allowing the fusion of streams of intelligence into a real-time common operating picture (COP)/common intelligence picture (CIP) (Stokes, et al. 2025, 2). Applied to nuclear deterrence, such systems could enhance situational awareness, threat assessment, and forecasting; however, they also risk overwhelming decision-makers or accelerating escalation cycles. DL expands these possibilities further by powering both **classification models**, which can identify objects, signals, or patterns from sensor data relevant to missile tracking and intelligence, surveillance, reconnaissance, and targeting (ISR-T), and **predictive models** that could refine early-warning, tracking or targeting processes. More recently, AI has introduced **generative models** capable of creating new content, such as text, imagery, simulations, or even adaptive so-called "AI advisors", which offer the possibility of real-time AI assistance in developing nuclear response options or simulating adversary strategies (Stokes, et al. 2025, 2-3). **Foundation models** represent a further technological advancement. Enabled with the introduction of transformer architectures since 2017, these large-scale, pre-trained deep learning systems can process massive quantities of multimodal data, capture complex relationships, and then be fine-tuned to specialize in specific domains. The flexibility of foundation models allows integration across classification, predictive, and generative functions, with potential applications ranging from advanced ISR-T to strategic planning simulations. However, their reliance on extensive datasets, computationally intensive training, and susceptibility to produce erroneous data, false outputs and a known tendency to "hallucinate", introduces novel risks in potential integration within nuclear deterrence processes, raising concerns about reliability, control, and the erosion of deliberate human oversight in the most sensitive of contexts, including the possible emergence of "black box" processes beyond the full knowledge or awareness of human operators (Chernavskikh 2024, 4, Protasov, Shirmanov and Radomanov 2023).

3. Artificial Intelligence in Modern and Future Nuclear Deterrence

Building on historical trends in the automation of vital functions of deterrence enabling processes, and considering the contemporary set of AI capabilities being offered, the following chapter examines some of the approaches of AI implementation into the larger nuclear balance and explores the evolution of the impending AI-nuclear nexus. Two specific subsets or vectors of development are presented – the more probable, relating to low-risk and attainable points of AI integration in the near future, which could have a limited impact on deterrence; the less probable, pertaining to two possible scenarios of expansive AI integration into either strategic offensive strike potential or strategic defensive capabilities (i.e. missile defense). Both scenarios, however, are examined as possessing a far greater degree of negative potential in undermining future deterrence over the medium to long term.

In the assessment of current developments, scientific thought and research being publicly disseminated, the strive towards integration of AI is widely recognized as a necessary advancement, with the key limitations of maintaining established "human in the loop" controls. Within Western literature, near-term applications of AI are seen as a continuation of preceding efforts, namely the incorporation of improvements to NC3 and ISR-T subsystems, where AI could serve as a significant capability enhancer, with a future set of capability enablement, once AI technologies have matured enough and have been tested within deterrence architecture. More specifically, focus is placed on improving ISR-T capabilities through a fusion of sensor data within AI matrices, thereby providing human operators with a more precise overall picture at expedited timeframes. Thus, the detection, early warning and response chains could be vastly improved, reinforcing deterrence. Furthermore, complex predictive and simulation AI models are seen as an improved measure to provide simulation studies and, thus, test both hypothetical adversary capabilities, but more importantly, own response measures (Boulanin, et al. 2019, Horowitz, Scharre and Velez-Green 2019, Stokes, et al. 2025). Overall, the integration of artificial intelligence (AI) into nuclear deterrence systems presents a complex array of both stabilising and destabilising effects, which together fundamentally challenge traditional deterrence paradigms. In one subset of examined functions of nuclear deterrence, AI possesses significant transformative potential for ISR-T, as well as NC3 capabilities, enhancing early warning, threat detection, and decision support. By processing vast and complex flows of sensor data rapidly and with greater accuracy, AI can reduce false alarms and bolster the reliability of second-strike capabilities, thereby strengthening deterrence credibility (Chernavskikh 2024, Schwartz and Horowitz 2025). However, the compression of decision-making cycles caused by AI acceleration poses serious risks, especially in the conditions of a "launch on warning" posture.

In the offensive side of the AI-nuclear nexus, the prospects for integrating AI within specific platforms and delivery systems are examined. Specifically, within Russian military thought and theory, the aspects of semi- or fully autonomous AI-driven systems are placed as focal points of future deterrence. This is particularly evident within the operations of certain systems such as the 9M39 Poseidon unmanned underwater nuclear-powered strategic nuclear system and the prospective 9M730 Burevestnik intercontinental nuclear-powered cruise missile – with both systems projected to have varying degrees of automation (Fatter 2020). Russian strategic thinking views such systems as affording an assured second-strike capability in the context of potential degradation of the effectiveness of the traditional nuclear triad, and the implementation of AI technologies is seen as a key enabler.

Within the more mundane aspects of nuclear deterrence and nuclear forces operations, the permeation of AI technologies is also observed. In the context of the Russian Strategic Rocket Forces, the complexity of introduced modern systems places the requirements for high-quality technical support, with the reliability of new systems not significantly reducing maintenance demands or failures, which in turn increases workload on support officers and technicians. With the complexity of systems increasing exponentially, both horizontally and vertically within the force structure and beyond to other connected sectors, the day-to-day operations and reliability of nuclear deterrence forces are placed under increased strain. Thus, AI automation is presented as a necessary step to maintaining readiness under heavy informational and operational burdens. The proposed Technical Support System (TCO), which appears to be at a certain limited levels of introduction includes AI process integration across management organs (control points, command structures), automated command-and-control (C2) systems, support units, and extending to the demands forwarded to defense industry enterprises with the main goal being to maintain readiness of missile units by ensuring the supply of technical components, data, instructions, reports of problems and the communication of changing operational requirements (Skiba, Kovalev and Brizhan 2022).

3.1. Strategic Offensive and Defensive AI Dominance

Beyond the probable scenarios of AI implementation previously discussed, several others are also presented. The scenarios take the assumption of expansive AI integration across multiple system levels and the handing of either direct control or the placement of extreme trust in AI proposed solutions. Both scenarios presented would have extremely detrimental effects for nuclear deterrence, as they would constitute an entirely new centre of gravity within the strategic nuclear balance. Perceived superiority in offensive and/or defensive capabilities could enable a potential effective first-strike scenario or could elicit adversaries to conduct pre-emptive strikes. The broader scientific consensus opposes the proposed scenarios, as they would, as previously stated, lead to extreme, unpredictable, and difficult-to-manage changes in the nuclear balance and the erosion of deterrence.

In the first scenario centred on an AI-driven offensive edge, the prospects for an effective first-strike scenario are explored. Under this scenario, AI is utilized to provide solutions where the entirety or vast majority of an adversary's retaliatory potential, both conventional and nuclear, is neutralized, the so-called "splendid first strike" (Geist 2023, 193). AI is explored as an instrument, integrated across NC3 and ISR-T architectures, which can significantly degrade the survivability of an adversary's retaliatory capacity. An example, often provided, is the theoretical ability for AI-driven processes to fuse vast amounts of incomplete or otherwise ambiguous sensory data to detect and track the locations of highly survivable assets such as SSBNs or ICBM transporter-erector-launchers (TELs) and, thus, provide location and targeting solutions for their neutralization in a coordinated strike (Chernavskikh 2024, 5, Johnson, Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age 2022, 348-349). Elevated further, the proposition is made that AI could enable, through vast simulations, an attack scenario, which circumvents an adversary's ability to effectively retaliate (Fatter 2020). Fully AI-enabled strategic offensive nuclear capabilities would, thus, fundamentally challenge the architecture of nuclear deterrence by endangering the assured second-strike capability and the primacy of human control. The full-scale deployment or the credible perception of such a scenario as imminent could catalyse pre-emptive strategies, accelerate crisis dynamics, degrade decision-making quality, and become the harbinger for a further destabilizing arms race in offensive and defensive AI systems through perceived AI capability gaps. The possible integration of AI into offensive strategic potential is inseparable from advances in defensive systems, creating a dynamic of escalating strategic competition. Major powers seeking to maintain credible deterrence under an increasingly AI-driven strategic environment are likely to invest heavily in AI-enabled defense architectures, which themselves pose substantially similar challenges for deterrence.

The second scenario examines the concept of AI-driven strategic defensive systems. Chiefly, the focus is placed on the ability of a strategic missile defense system to effectively counter an adversary's full-scale strike. Some elements of such a prospective AI-enabled capability derive from the previously discussed offensive AI edge, such as the ability to track in advance certain mobile and hard-to-detect offensive assets. Other elements focus on AI-driven interception of attack vectors, which is traditionally complicated by a number of factors – tracking and telemetry of an incoming strike, differentiation between warheads and decoys, overcoming electronic measures (EW) measures, targeting and guidance of own interceptor assets, retargeting in case of failed interceptions (Saveleev 2023). The increased potential of offensive means, such as maneuverable exo- or endo-atmospheric hypersonics, combined in the future with on-board AI-driven guidance presents further challenges (Fatter 2020), which AI has the potential to provide a solution for – an example of this is the extremely difficult to predict (random) changes in the flight path of legacy maneuverable re-entry vehicles or novel hypersonic glide vehicles. In a hypothetical scenario, an AI-driven and controlled system, supplied with sufficient strategic and operational assets, from sensory to kinetic effectors, could be capable of efficiently coordinating defensive measures, with fewer resources and within a shorter timeframe than current systems. The effects of such AI-enabled strategic defensive superiority on nuclear deterrence would be both significant and double-edged. On one hand, an effective missile defense system capable of reliably intercepting incoming missiles could undermine the doctrine of assured retaliation that lies at the heart of deterrence theory. If one side comes to the acceptance that it can successfully neutralize most or all of an adversary's retaliatory potential, the mutual vulnerability essential to deterrence could be eroded. Conversely, under the conditions of an own "no first strike" policy, a credible AI-enhanced missile defense could also serve as a stabilizing factor, by raising the costs and risks of offensive nuclear strikes, thereby dissuading adversaries from initiating conflict (Saveleev 2023).

Regardless, some key considerations arise regarding the overarching processes of technological incorporation into the security field, especially when considering a novel technological layer with many variables. Such considerations extend beyond AI itself and align with general procedures and best practices in military technology integration. The introduction of new technology into the broad set of systems in the military field is an expansive and time-consuming process, where a given technological instrument or piece of equipment may require many years of testing and evaluation to ensure its performance, resilience, availability, and that potential shortcomings meet ever-changing requirements and parameters – examples of such cases can be found in the level of processing power used in units of otherwise modern military equipment, where technology is generations behind what is available for commercial processors; to an even greater degree, the successive iterations and improvements of SACCS utilized floppy disks well into the twenty-first century in order to ensure system reliability and survivability (Boulanin, et al. 2019). General challenges associated with the full potential of AI, such as physical limitations of processing capacity in individual units of equipment, or overconcentration in singular hubs, as well as the increasingly vast power requirements for the functioning of advanced AI models also weigh in heavily in considerations about the mass integration of AI. The potential critical vulnerabilities associated with such expansive additions to overall nuclear deterrence capabilities further underline a potentially slower and more limited scope of future incorporation.

In examining certain cases of future evolution of deterrence, AI can be conceptualized as a threat to the survivability of second-strike capabilities by enhancing the tracking and targeting of survivable assets, such as SSBNs and TELs. This degradation of assured retaliation could motivate an effective first strike scenario, adversary pre-emptive strikes or facilitate changes in nuclear postures (Chernavskikh 2024, Fatter 2020). Overall, AI-enabled effective first-strike capacity and advanced missile defense capabilities introduce destabilizing incentives by eroding the cornerstone of nuclear deterrence expressed in mutual vulnerability. The perceived possibility of neutralizing an adversary's retaliatory capacity may prompt aggressive strategies and undermine crisis stability. This creates a security dilemma as states escalate both offensive and defensive AI applications, thereby increasing strategic uncertainty and distrust (Horowitz, Scharre and Velez-Green 2019, Schwartz and Horowitz 2025, Fatter 2020). As the AI-nuclear nexus expands and attracts ever greater attention and resources perceived capability gaps, an "AI gap", could develop and erode deterrence in similar ways to past instances of Cold War-era capability uncertainty. Despite these risks, the scholarly consensus suggests outcomes depend heavily on policy decisions and governance frameworks (Stefanovich 2019). Retaining human control over nuclear use while leveraging AI's analytical advantages is crucial. Clear international norms and transparency can also assist in risk mitigation and harness AI's stabilizing potential to bolster deterrence through improved situational awareness and system reliability (Stokes, et al. 2025, Scharre and Depp 2024, Dooling 2025).

Conclusions

The convergence of artificial intelligence and nuclear deterrence represents both a continuation of Cold War–era processes of automation and a qualitative transformation of deterrence in the twenty-first century. Historical vectors of development from the Cold War demonstrate that automation has long been integral to maintaining credible deterrence. However, the context of modern AI approaches and models introduces a far more complex technological layer. Rule-based AI has already proven its utility in early-warning and secure communications, while machine learning and deep learning promise to enhance classification, prediction, and decision-support across ISR-T and NC3. More recently, the development of transformer-based foundation models suggests the possibility of highly generalizable AI systems, able to fuse multimodal data and provide real-time support for strategic decision-making. These advances hold the potential to reinforce deterrence through improved resilience, accuracy, and situational awareness.

Nevertheless, the same capabilities may destabilize the strategic nuclear balance and undermine deterrence. The acceleration of decision-making cycles, the opacity of "black box" models, and the possibility of false outputs or "hallucinations" raise profound risks. Concurrently, the integration of AI into offensive systems, or into strategic missile defense architectures threaten to erode the mutual vulnerability upon which deterrence rests. A credible AI-enabled first strike or effective defensive shield could undermine assured retaliation, encourage pre-emption, or entice a first-strike scenario. Furthermore, the emergence of an "AI gap" between nuclear powers could replicate the uncertainty and arms race dynamics of prior eras, heightening mistrust and strategic competition.

The analysis thus underscores an unfolding security paradox – AI may bolster deterrence by reducing uncertainty and enhancing second-strike reliability, but also risks undermining stability, if integrated in ways that compress human interaction and oversight or alter significantly the balance between offensive and defensive capabilities. What ultimately matters are the choices states make in adopting, constraining, and governing AI applications in nuclear systems and whether future approaches towards maintaining a strategic nuclear balance synchronize across major global powers, similarly to preceding historical processes of nuclear deterrence provision. Retaining meaningful human control, ensuring transparency, and developing international norms or informal models of mutual understanding will be decisive in mitigating risks. In this respect, AI should be seen not as an inevitable destabilizer or guarantor of stability, but as a contingent variable – its impact will depend on the policies, doctrines, and safeguards that accompany its deployment. How the major nuclear powers of the U.S.A., Russia and China manage the AI–nuclear nexus will determine whether AI becomes a stabilizing force reinforcing deterrence, or a disruptive catalyst for renewed instability.

BIBLIOGRAPHY:

Akiyama, Nobumasa. 2021. "AI Nuclear Winter or AI That Saves Humanity? AI and Nuclear Deterrence". *Robotics, AI, and Humanity: Science, Ethics, and Policy* (Springer) 161-173. doi:https://doi.org/10.1007/978-3-030-54173-6.

Boulanin, Vincent, John Borrie, Page Stoutland, and Petr Topychkanov. 2019. *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk.* Solna: SIPRI, 41-55.

Chernavskikh, Vladislav. 2024. *Nuclear Weapons and Artificial Intelligence: Technological Promises and Practical Realities.* SIPRI Background Paper, Solna: SIPRI.

Deepgram. 2025. *Rule-Based AI.* May 8. Accessed September 5, 2025. https://deepgram.com/ai-glossary/rule-based-ai

Dooling, Maria. 2025. *Develop a Risk Assessment Framework for AI Integration into Nuclear Weapons Command, Control, and Communications Systems.* FAS. June 11. Accessed September 10, 2025. https://fas.org/publication/risk-assessment-framework-ai-nuclear-weapons/

Fatter, E. 2020. *Iskusstvennyj intellekt, avtomatizacija i jadernaja stabil'nost': na puti k bolee slozhnomu jadernomu budushhemu.* Valdai Club. October 15. Accessed September 7, 2025. https://ru.valdaiclub.com/a/highlights/iskusstvennyy-intellekt-i-yadernaya-stabilnost/

Фаттер, Э. 2020. *Искусственный интеллект, автоматизация и ядерная стабильность: на пути к более сложному ядерному будущему.* October 15. Accessed September 7, 2025. https://ru.valdaiclub.com/a/highlights/iskusstvennyy-intellekt-i-yadernaya-stabilnost/

Federation of Atomic Scientists. 1999. *https://nuke.fas.org/guide/usa/c3i/saccs.htm.* January 10. Accessed September 3, 2025. https://nuke.fas.org/guide/usa/c3i/saccs.htm

Geist, Edward. 2023. *Deterrence under Uncertainty: Artificial Intelligence and Nuclear Warfare.* Oxford University Press. doi:10.1093/oso/9780192886323.001.0001.

Goodfellow, I., Y. Bengio, and A Courville. 2016. *Deep Learning.* MIT Press.

Horowitz, Michael C., Paul Scharre, and Alexander Velez-Green. 2019. *A Stable Nuclear Future? The Impact of Autonomous Systems and Artificial Intelligence.* Cornell University. Accessed September 4, 2025. doi:https://doi.org/10.48550/arXiv.1912.05291

Jensen, Benjamin, Yasir Atalan, and Jose M. Macias III. 2024. *Algorithmic Stability: How AI Could Shape the Future of Deterrence.* Center for Strategic and International Studies. Accessed September 8, 2025. https://www.csis.org/analysis/algorithmic-stability-how-ai-could-shape-future-deterrence

Johnson, James. 2020. “Deterrence in the age of artificial intelligence & autonomy: a paradigm shift in nuclear deterrence theory and practice?” *Defense & Security Analysis* 36 (4): 422–448. doi:10.1080/14751798.2020.1857911

Johnson, James. 2022. “Inadvertent escalation in the age of intelligence machines: A new model for nuclear risk in the digital age.” *European Journal of International Security* 7: 337–359. doi:10.1017/eis.2021.23

LeCun, Y., Y. Bengio, and G. Hinton. 2015. “Deep Learning.” *Nature* 521: 436–444.

Mitchell, T. M. 1997. *Machine Learning.* McGraw-Hill.

MITRE Partnership Network. n.d. *SAGE Semi-Automatic Ground Environment First MITRE Work Program.* Accessed September 4, 2025. https://sage.mitre.org/

Protasov, A.A., A.V. Shirmanov, and S.I. Radomanov. 2023. “Tehnologicheskie razrbotki v oblasti izkusstvennogo intelekta i sderzhevanie potencial’nogo agresora.” *Voennaja myslja* 11: 68-83.

Протасов, А.А., А.В. Ширманов, и С.И. Радоманов. 2023. “Технологические разрботки в области изкусственного интелекта и сдержевание потенциального агресора.” *Военная мысль* 11: 68-83.

Saveleev, A.G. 2023. “Jadernoe sderzhivanie, strategicheskaja stabil’nost’, protivoraketnaja oborona: Dajot li jadernyj arsenal podlinnuju bezopasnost’ gosudarstvam.” *Russia in Global Politics* (Russia in Global Politics) 21 (5): 20-34. doi:10.31278/1810-6439-2023-21-5-20-34

Савельев, А.Г. 2023. “Ядерное сдерживание, стратегическая стабильность, противоракетная оборона: Даёт ли ядерный арсенал подлинную безопасность государствам.” *Россия в глобальной политике* (Россия в глобальной политике) 21 (5): 20-34. doi:10.31278/1810-6439-2023-21-5-20-34

Schance, John. 1998. *465L WEAPON SYSTEM STRATEGIC AUTOMATED COMMAND CONTROL SYSTEM (SACCS).* January 15 . Accessed September 3, 2025. https://nuke.fas.org/guide/usa/c3i/cvpmrjan/index.htm

Scharre, Paul, and Michael Depp. 2024. *Artificial Intelligence and Nuclear Stability.* CNAS. January 16. Accessed September 10, 2025. https://www.cnas.org/publications/commentary/artificial-intelligence-and-nuclear-stability

Schwartz, Joshua A., and Michael C. Horowitz. 2025. *Out of the Loop: How Dangerous is Weaponizing Automated Nuclear Systems?* Cornell University. Accessed September 5, 2025. https://arxiv.org/pdf/2505.00496

Science Direct. n.d. *Rule-Based System.* Accessed September 5, 2025. https://www.sciencedirect.com/topics/engineering/rule-based-system?

Skiba, V.A., A.M. Kovalev, and A.S. Brizhan. 2022. "Osobennosti avtomatizacii processov funkcionirovanija sistemy upravlenija tehnicheskim obespecheniem Raketnyh vojsk strategimeskogo naznachenija." *Voennaja myslja* 10: 51-58.

Скиба, В.А., А.М. Ковалев, и А.С. Брижан. 2022. "Особенности автоматизации процессов функционирования системы управления техническим обеспечением Ракетных войск стратегимеского назначения." *Военная мысля* 10: 51-58.

Stefanovich, D. 2019. *Iskusstvennyj intellekt i jadernoe oruzhie.* Analytical Report, Moscow: Russian Council on Foreign Relations: RSDM. Accessed September 5, 2025. https://russiancouncil.ru/analytics-and-comments/analytics/iskusstvennyy-intellekt-i-yadernoe-oruzhie/

Стефанович, Дмитрий. 2019. *Искусственный интеллект и ядерное оружие.* Аналитические статьи, Москва: Российский совет по международным делам: РСМД. Accessed September 5, 2025. https://russiancouncil.ru/analytics-and-comments/analytics/iskusstvennyy-intellekt-i-yadernoe-oruzhie/

Stokes, Jacob, Colin H. Kahl, Andrea Kendall-Taylor, and Nicholas Lokker. 2025. *Averting AI Armageddon: U.S.-China-Russia Rivalry at the Nexus of Nuclear Weapons and Artificial Intelligence.* Washington, DC: Center for a New American Security.

Tobey, J. R. 1959. *Basic XD-1 Information: Introduction to SAGE and XD-1.* Technical Memorandum , Lexington: MITRE Corporation.

US Department of Defense. 2020. *Nuclear Matters Handbook.* Accessed September 8, 2025. https://www.acq.osd.mil/ncbdp/nm/NMHB2020rev/chapters/chapter2.html

Yarynich, Valery E. 2003. *C3: Nuclear Command, Control Cooperation.* Washington, D.C.: Center for Defense Information.