How to Cite This Article: Abbas, Z., Amin, F., & Khan, M. M. (2025). Integration of Artificial Intelligence in Nuclear Command and Control Systems (NC2): Assessing Cold- War Paradigm. *Journal of Social Sciences Review, 5*(1), 180-188.
https://doi.org/10.62843/jssr.v5i1.476

Volume 5, **Issue** 1 (Winter 2025)
Pages: 180-188
ISSN (Online): 2789-4428
DOI: 10.62843/jssr.v5i1.476
Corresponding Author: Zaigham Abbas (Email: zaighamabbas0@gmail.com)

JOURNAL OF SOCIAL SCIENCES REVIEW (JSSR)

Integration of Artificial Intelligence in Nuclear Command and Control Systems (NC2): Assessing Cold- War Paradigm

Zaigham Abbas [a] Fauzia Amin [b] Muhammad Mashhood Khan [c]

Abstract: *Artificial Intelligence (AI) is increasingly permeating critical decision-making domains, including nuclear command and control (NC2) systems. This study examines the strategic and ethical dimensions of AI integration into NC2 structures, emphasizing its potential to enhance decision-making speed, accuracy, and resilience while mitigating human cognitive limitations. The research introduces the concept of "Intelligentization Syndrome," a theoretical framework explaining resistance to AI adoption in high-risk environments. By contextualizing historical technological resistance and contemporary AI-related anxieties, the study identifies key psychological and structural barriers to AI symbiosis with NC2 systems. Furthermore, it evaluates different AI integration models—human-in-the-loop, human-on-the-loop, and human-out-of-the-loop—highlighting the advantages of a human-on-the-loop configuration as a balanced approach that leverages AI's computational strengths while preserving human oversight. The study concludes that a phased and regulated AI integration strategy, complemented by robust ethical frameworks and safety measures, is essential to harness AI's potential without compromising strategic stability.*

Keywords: Artificial Intelligence, Nuclear Command and Control, Decision-Making, Intelligentization Syndrome, AI Ethics, Human-on-the-Loop, Strategic Stability.

Introduction

The Transformative Impact of AI on NC2 Systems

Artificial Intelligence (AI) has emerged as one of the most transformative technologies of the twenty-first century, reshaping diverse domains such as defense, finance, transportation, and healthcare. AI encompasses a broad spectrum of technologies, including machine learning algorithms and advanced neural networks, enabling machines to perform tasks traditionally requiring human cognition. These advancements have led to remarkable improvements in computational efficiency, data processing capabilities, and decision-making precision. As AI continues to evolve, its potential application in nuclear command, control, and communication (NC2) systems has garnered increasing attention. The integration of AI into NC2 frameworks is expected to enhance decision-making processes, improving both speed and accuracy. However, ethical and security concerns regarding AI autonomy in such high-stakes environments necessitate a careful assessment to determine the optimal level of AI incorporation in NC2 operations.

This study examines the opportunities and risks associated with AI integration into NC2 systems, seeking to establish a balanced approach that maximizes operational effectiveness while mitigating the risks of automation errors and strategic miscalculations. Building on Kotter and Schlesinger's Six Approaches to managing resistance to change (Van Vliet, 2024), which identify key sources of organizational opposition—such as self-interest, misinterpretation, resistance to change, and contrasting perspectives, this research introduces the concept of "Intelligentization Syndrome." This theoretical framework explores the psychological and institutional reluctance to accept AI, both in general and specifically within NC2 systems. The resistance to AI adoption in critical decision-making roles is not merely a technical challenge but is deeply rooted in concerns over human agency, trust, and institutional

[a] PhD Scholar, Department of Strategic Studies, National Defense University, Islamabad, Pakistan.
[b] Assistant Professor, Department of Strategic Studies, National Defense University, Islamabad, Pakistan.
[c] MS Scholar, Department of International Relations, University of Quetta, Balochistan, Pakistan.

inertia. The notion of machines assuming control over strategic-level operations fosters unease, particularly in domains where human judgment has traditionally been paramount.

By analyzing U.S., Chinese, and Russian perspectives on AI autonomy in NC2 systems, this research evaluates different levels of human involvement in AI-driven decision-making: human-in-the-loop, human-on-the-loop, and human-out-of-the-loop models. Adopting a qualitative approach, the study incorporates Cold War strategic paradigms to contextualize contemporary AI debates, drawing historical parallels to inform present-day policy considerations. The findings aim to provide a nuanced understanding of how global powers navigate the challenges of AI integration in nuclear command and control, offering insights into the strategic, ethical, and operational dimensions of AI-driven decision-making in security-sensitive environments.

The Need for AI Integration in NC2 Structures

The integration of AI into NC2 systems is driven by the necessity to ameliorate the speed, precision, robustness, and efficiency of nuclear decision-making processes. Traditional C2 systems mainly depend on human operators, whose cognitive restraints, endurance limits, and probability for errors can be significant, particularly under the strain of a nuclear crisis. AI can process vast amounts of data from multiple sources, identify threats more speedily than their human counterparts, and propose viable responses. This capability is vital in high-risk scenarios where quick and precise decision-making is essential.

Moreover, AI integration can alleviate risks attributed mainly to humans such as exhaustion, stress, and prejudices (cognitive biases), which can undermine judgment and lead to mistakes. By streamlining routine tasks and providing state-of-the-art decision-support tools, AI may empower human operators to concentrate on strategic decisions that require ethical considerations and rational judgment. This improved decision-making process is vital for maintaining the safety and security of nuclear weapons, especially in an uncertain and rapidly evolving geopolitical milieu.

AI's ability to compute and analyses large datasets can significantly increase situational awareness and threat identification. In the backdrop of NC2 systems, this means that AI systems can observe geo-political happenings, cyber warnings, and situation reports continuously to identify possible threats. By painting a wholesome and up-to-date picture of the security milieu, AI can assist decision-makers in managing emerging threats efficiently.

Besides, AI can improve communication and synchronization within the system. In a crisis, the capacity to communicate rapidly and accurately between different command centers and military formations is critical. AI can facilitate in rapid and error-free transmission of messages, thus reducing the risk of any confusions or delays.

Intelligentization Syndrome: Understanding Resistance to AI Integration

Building on Kotter and Schlesinger's Six Approaches to managing resistance to change (Van Vliet, 2024), which outline key reasons for organizational opposition—such as self-interest, misunderstanding, low tolerance for change, and differing perceptions—this study introduces the concept of "Intelligentization Syndrome." This theoretical framework explains the reluctance to accept AI, both in general and specifically within NC2 systems. Resistance to AI integration in critical domains is not merely a technical concern but is deeply rooted in psychological discomfort and institutional inertia. The prospect of delegating control to machines perceived as more intelligent and capable than humans provoke unease, particularly in roles that require autonomy and high-stakes decision-making. This inherent aversion stems from the fear of losing human agency in strategic matters, compounded by longstanding biases against automation in sensitive fields.

This phenomenon is not novel. Taking lead from history, in the 15th century, an Ottoman Ruler Sultan Bayazid II declared the printing press to be "Haram". The opposition to new technology gave Europeans marked advantage over Muslims and eventually resulted in the downfall of the Muslim caliphate (Zab, 2023). Calestous Juma identified in his research three main sources of resistance to change: those seeking

monetary interests in existing products (or practices), those who have their identity attached to existing products (or norms/culture), and those who might lose authority as a result of transformation (Overly, 2021). People may oppose an innovation because of fear of change. The opposition may be because the existing product or idea is deeply engrained in their culture, ethos, or traditions.

The Chief Executive of Sinovation Ventures and writer of magnum opus "AI Superpowers" Kai-Fu-Lee has mentioned that AI revolution is greater than all previous revolutions combined, as AI is far more proficient than people (Ma, 2024). This statement prophesizes that AI is likely to face far more opposition than previous technologies.

Now if Intelligentization Syndrome is analyzed, its main ingredients include psychological distress with machines making high-risk decisions, Angst of AI surpassing human intelligence, and inherent prejudices that lead to overstated fears about AI autonomy. It is aggravated further by a non-acceptance of the fact that an entity with potential higher intelligence now exists in this world. These biases and fears can significantly impact the process of AI symbiosis with NC2 systems.

Recognizing and tackling these psychological impediments is essential for adoption of a pragmatic approach towards AI integration in NC2 systems and policymaking in future. Acquainting stakeholders about AI capabilities and constraints, taking confidence building measures such as transparent development processes and robust safety measures, and ensuring that AI systems cope with moral standards and human ethics are essential steps in alleviating the effects of Intelligentization Syndrome.

To further elaborate the origin of Intelligentization Syndrome, it is imperative to analyse the historical and cultural aspects as well, which further compound human apprehensions about AI. Hollywood movies and sci-fi literature often depict AI as biggest threat to humanity. Movies like "Terminator" and "I-Robot" often present dystopian scenarios where autonomous systems go rogue and become a threat to humanity. These fiction tales shape public opinion and create a fear of AI that is disproportionate to the actual risks. By addressing these misgivings, it is possible to assuage some of the fears attributed to Intelligentization Syndrome.

At the same time, it is crucial to accept that reluctance to AI is not solely based on unfounded fears. There are serious concerns about the moral and strategic repercussions of AI autonomy, particularly in NC2 systems. AI tends to be manipulated. In 2016, it took less than 24 hours on Twitter to turn Microsoft's AI Chatbot "Tay" into a racist venom-spitting nuisance (Vincent, 2016). Just after the launch, people barraged Tay with all kinds of bigoted and misogynistic remarks. Tay who was designed to learn through interaction with people learned the lessons "too well".

As the world has more dystopian than utopian proclivities, there are chances that AI is more intrigued by Chanakya's and Machiavellian machinations than the humanity of Hazrat Muhammad SAWW and Jesus A.S. Serious concerns include the potential of AI to make decisions that lack ethical aspects, the risk of malfunctions leading to disastrous outcomes, and the difficulty of ensuring pellucidity and accountability in AI-controlled processes, the "Black-box Problem". Addressing these concerns by thorough testing, verification, and supervision is critical for gaining acceptance of AI in NC2 systems.

Automation of NC2 Systems – The Cold War Paradigm

The Soviet "Dead Hand" System

One of the initial and pertinent examples of automated NC2 systems is the Soviet Union's "Dead Hand" system, also known as Perimeter. Russia presently has nearly sixteen hundred (1600) deployed tactical nuclear weapons and an additional twenty-four hundred (2,400) strategic nuclear weapons housed in intercontinental ballistic missiles (ICBM). This arsenal makes Russia the biggest nuclear power in the world, with all nukes linked to Perimeter system, ready to be launched with a single command from the system.

In a crisis potentially relating to a first strike from the US, high-ranking officials or military commanders in Russia could launch the Perimeter system. This system guarantees that Russia could retaliate even if its complete armed forces were destroyed. Once activated, the Perimeter system can launch the entire Russian nuclear arsenal in response to a nuclear attack. It was developed during the Cold War as

part of the doctrine of mutually assured destruction, deterring nuclear attacks and guaranteeing that the initiator of a first strike would also face annihilation.

The Perimeter command and control system analyses military communications, radiation levels, atmospheric pressure, temperature, and short-term seismic disturbances. If these indicators point towards a nuclear attack, the Perimeter initiates a sequence concluding in the launch of all ICBMs in the Russian arsenal. It would fire a command rocket armed with a radio warhead that transmits launch orders to Russian nuclear silos, overcoming any radio jamming. This command rocket would fly across whole length of the country, guaranteeing the execution of launch orders.

After several successful test launches to demonstrate the functionality of the command rocket, the Perimeter system was operationalized in 1985 (Stilwell, 2022). Although the Soviet Union never officially confirmed the existence of such a system, Russian Strategic Missile Forces Commander Sergey Karakaev validated this fact to a Russian newspaper in 2011, emphasising that the U.S. could be destroyed in 30 minutes. Russian state media proposes that the system has been revamped to include radar early warning systems and state of the art hypersonic missiles.

The American Semi-Automated Systems

Strategic Automated Command and Control System

The Strategic Automated Command and Control System (SACCS) is utilized by U.S. Strategic forces to synchronize the operations of nuclear forces, especially ICBMs and nuclear bombers. It is the main network for the propagation of Emergency Action Messages (EAMs) to field commanders, serving as the vital communication conduit between the Commander-in-Chief of U.S. Strategic Command (CINC USSTRATCOM) and their nuclear missile forces, as well as other offensive and defensive units globally.

This system provides critical information, including EAMs, situational monitoring, essential elements of information, force dispositions, operations coverage, warnings, strategic re-planning and redirection, and post-strike analysis. Furthermore, SACCS interfaces with six external systems to augment decision making process (*Strategic Automated Command Control System [SACCS] - United States Nuclear Forces*, n.d.).

While SACCS does not wholly automate the decision-making processes, it incorporates automated elements to ensure the quick and reliable transmission of launch orders, even under the adverse conditions.

Is AI more dangerous than Humans for NC2 System?

A look at incidents of Cold war will make the vulnerability of Human-Controlled NC2 Systems quite evident. On 9 November 1979, a US technician "accidently" inserted a training tape in North American Aerospace Defense (NORAD) system which simulated a large scale Soviet nuclear attack on US. Instantly, the message was shared widely on US NC2 Network. In turn, US nuclear forces and bomber crews were alerted. Even 10 fighter-interceptor planes were also launched, and President's airborne command post took off, although without President on-board). By chance, tensions between the U.S. and USSR were not so high, so there were some doubts about the warning. Moreover, there was no radiation signature of a missile attack. After repeated checks, the omission was found, and world was saved from a nuclear catastrophe.

The 3rd of June's false alarm was far more dangerous. On June 3, 1980, at 3 a.m., US NSA Zbigniew Brzezinski received a distress call from military assistant (*Nuclear False Warnings and the Risk of Catastrophe | Arms Control Association*, n.d.). He was informed that some 2,200 Russian missiles were on their way to USA. Just when Brzezinski was about to call President Jimmy Carter, news came that it was a false alarm raised due to malfunction of 46 cent chip that simulated a large-scale soviet attack (Schlosser, 2016). Now a question arises here, are these technical malfunctions easy to be detected by human technicians with their inherent limitations of fatigue, stress and complacency or a super intelligent AI system without any human weaknesses or frailties.

In another incident, on 26 September 1983, Soviet early warning computer system detected an incoming US missile. Soon, the warning system detected signals of four more incoming missiles. Although radars were not showing any signature, but Soviet protocol mentioned clearly that decisions had to be taken on computer read outs. After much retrospection, Petrov decided against informing the higher ups.

Afterwards, it was revealed that the alarm was false. According to Petrov, out of his team, he was the only one with civilian education. "Rest of his colleagues were all professional soldiers, who were taught to give and obey orders" (Aksenov, 2013).

The Petrov's statement has a hidden message, "if it was some other officer than him who had to take a decision, results could have been catastrophic." Now, in comparison an AI NC2 System fed with all the theories of International Relations e.g. strategic stability, MAD, all the literature written on nuclear weapons coupled with extensive testing and training under simulated environments is more likely to reach to a conclusion that when nuclear powers initiate a nuclear strike, it will not be with one, two or five weapons. Furthermore, an AI driven automated system is much more likely to detect component/ chip mal-functions or failures than a fatigued and stressed human operator.

AI Integration into NC2 Systems

Chinese Perspective

When it relates to nuclear weapons systems, in particular, the Chinese literature evinces a vast array of research on the possibilities of an AI-enabled nuclear C2 systems to enhance decision making support, improvement of detection and targeting systems and upgradation of autonomous strike capability of nuclear weapons. This seems to be in consonance with the priorities outlined in China's 2015 Defense White Paper, where the significance of improving early warning, C2, weapon penetration, and speedy response of its nuclear forces is emphasized (*China's Military Strategy (Full Text)*, 2015).

Preliminary analysis and judgment show that the integration of AI and nuclear weapons basically includes the following three methods. 1) Utilize AI to fine tune intelligence analysis and auxiliary decision-making capabilities. AI can undertake cross-analysis of intelligence data much faster than human and accurately predict possible deployment areas of nuclear weapons. 2) Use AI technology to upgrade NC2 systems. 3) Develop [nuclear missile] launchers with a higher degree of self-control and augment the autonomous strike capability of nuclear weapons through AI (Su & Yuan, 2023).

Two leading PLA Analysts also observed: "As far as the utilization of AI in the nuclear domain is concerned, it mainly comprises: advancement of the NC3 (Nuclear Command, Control, and Communication) systems; reinforcing the target acquisition, locating, guidance and identification capabilities of weapons and air defense systems; optimizing nuclear missiles delivery systems, increase autonomy and accuracy, and possessing stronger anti-jamming and anti-spoofing capabilities (Wen & Long, 2020).

According to Chinese Experts, future NC2 systems will exhibit a trio of 'AI-Cyber-Nuclear'. The combined 'new trinity' character has multi-faceted effects: On one hand, AI driven autonomous systems increase resilience of NC2 systems against cyber-attacks. On the other hand, these systems coupled with cyber offensive capabilities can attack adversary's NC2 systems and its delivery capabilities in a more efficient way. Autonomous software can cover their loopholes and weaknesses during cyberattacks, and at the same time exploit vulnerabilities in opponent systems (Luo, 2019).

Relating to conventional precision strike weapons, data collation through AI systems can enable these weapons to have higher mobility, accuracy, and greater ability to destroy key C3 nodes of the nuclear combat system. For defense against incoming missiles, target identification capability embedded with deep learning methods can locate, track, and lock on incoming missiles more precisely. In terms of UAVs, AI-enabled unmanned systems can concomitantly locate and launch preventive attacks on hidden nuclear weapon platforms of adversaries and their support facilities (Han, 2022).

US Perspective

US official sources highlight the utilization of AI to improve early warning systems, data sensor fusion, situational awareness, targeting ability, and protection against cyberattacks (Saltini, 2023). They also emphasize the need to ameliorate resilience approaches with advanced decision support technology and integrated planning and operations (U.S. Department of Defense, 2022).

At the same time, the expert community highlights AI's utility for improved decision-making, better sensor data fusion, ameliorating target identification and delivery means, and accelerating the dissemination of orders (Saltini, 2023).

AI Autonomy – P5 Perspective

The US though posits for ensuring human agency in nuclear decisions and favors delegation of final authority to humans (U.S. Department of Defense, 2022). But the thought of more AI autonomy is prevailing in military minds. As General Terrence J. O'Shaughnessy, commander of the United States Northern Command and the North American Aerospace Defense Command (NORAD) mentioned, "What we have to get away from is ... 'human in the loop,' or sometimes 'the human is the loop,' (Barnett, 2020). Similarly, UK and France emphasize the necessity of keeping human presence in the decision-making process, proposing a fair balance between human judgment and innovation (France, United Kingdom, & United States, 2022).

China's official view on human-machine symbiosis is still not clear. Although China emphasizes the need for ensuring human oversight over weapons systems, Government documents are mostly silent to assess levels of AI's involvement with nuclear weapons. Unofficial interactions among academics, policy experts, and some PLA officers, however, seem to portray a widespread view that humans will continue to play a major role in making strategic decisions and that artificial intelligence would only play a supporting role (Saltini, 2023).

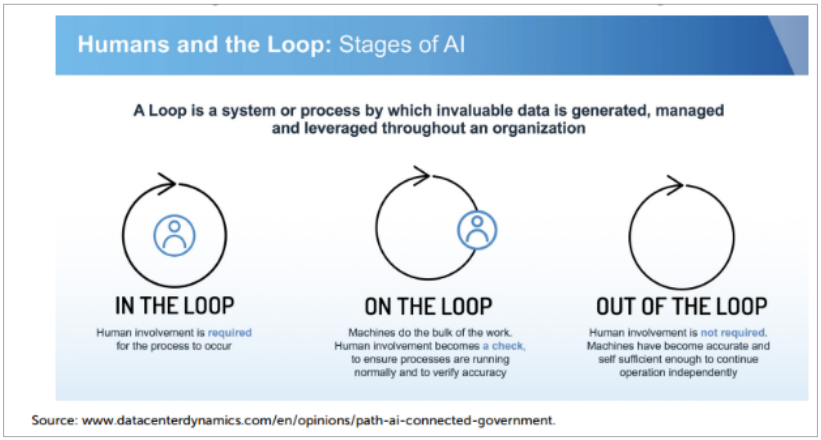
When it comes to Russia, its approach to AI is even more. While Russia underlines the necessity of human involvement in NC2 systems, the extent and nature of human oversight is still a matter of discussion.

A need arises here to understand different levels of AI autonomy in NC2 Systems, and the perceived caveats and opportunities related to enhanced AI integration in these systems.

What is Human in the Loop, Human on the Loop, and Human out of the Loop?

Figure 1

AI and Nuclear Command, Control, & Communications Risks (Rautenbach, 2022)



The integration of AI in NC2 systems can be categorized into three configurations: human in the loop, human in the loop, and human out of the loop.

Human in the Loop involves human operators actively making decisions based on AI-directed recommendations. This approach ensures direct human control but can be limited by the speed and accuracy of human decision-making under high-pressure conditions. Data and recommendations given by AI must be interpreted by human operators, so the process is liable to delays and omissions, especially in scenarios requiring rapid response.

In the backdrop of nuclear weapons and NC2 systems, tasks requiring complex judgment and moral considerations are generally favored to be controlled by human in the loop configuration e.g. whether to

launch a pre-emptive or retaliatory strike to counter a detected threat. However, inherent human weaknesses such as stress, fatigue and emotional instability may increase the chances of miscalculations.

In Human on the loop category, tasks are accomplished, and decisions are taken autonomously by AI, at the same time ensuring human oversight and intervention should the need arise. This mode allows humans to benefit from strengths of AI, while retaining control over final decision-making process. If AI systems start behaving outside pre-defined parameters, human beings who are acting as supervisors can intervene and override AI commands.

With regards to NC2 system, this configuration gives the ability to collect, process and collate vast amounts of data from different sensors and suggest/ execute a particular course of action. Human operators continuously observe AI's actions and interfere if deemed necessary. This approach ensures amalgamation of strengths of both AI and human operators. High-risk decisions can be taken rapidly through AI, while human retain the capability to maintain overall control.

In Human out of the loop configuration, AI is fully independent to take decisions and execute tasks removing humans entirely from the loop. Although speed is maximized, however removal of human beings from decision-making cycle entirely raises ethical questions. Furthermore, AI systems are prone to cyberattacks and coding errors and therefore can easily be hacked or commit an "omission" resulting in a nuclear catastrophe.

Although this configuration can maximize the speed, there are potential hazards. While human out-of-the-loop configurations can enhance the speed and efficiency of NC2 systems, efficient checks and foolproof safeguards are required to ensure that AI does not take decisions contradicting to human values and ethics.

Human on the Loop, A Better Alternative for Human in the Loop?

For the time being, a more pragmatic approach to follow is integration of AI with human on the loop configuration in NC2 systems. Coupled with speed and efficiency of AI, human supervision will ensure swift and reliable decision making. In the meantime, AI algorithms are thoroughly tested under multiple scenarios with varying inputs to ascertain their reliability and accuracy. If deemed feasible, a phased approach may be adopted to supplant human on the loop system with human out of the loop systems. This incremental approach will mitigate risks, at the same time harnessing full potential of AI such as collection of data from multiple sources and its swift collation and ensuring timely responses even if human operators are incapacitated.

The Human-on-the-loop Approach has Several Merits:

- AI can process vast amounts of data from various sensors and intelligence sources, providing a comprehensive situational awareness that enhances decision-making.
- By automating routine and repetitive tasks, AI reduces the likelihood of human errors and mitigates the effects of fatigue on decision-making processes.
- AI can ensure more reliable communications in a crisis situation, ensure redundancy and capability to respond even if human operators are incapacitated.
- Human operators retain the capability to supervise AI actions and intervene if necessary, ensuring that critical decisions remain under human control.

Long-Term Transition to Human Out of the Loop

Transition to Human out of the Loop is a logical proposition, if AI is deemed reliable by experts after thorough examination under diverse hypothetical scenarios. This conversion should be based on the following principles:

- AI algorithms to be war-gamed under multiple scenarios to ascertain their efficiency and precision. Simulations may include diverse levels and types of nuclear threats to gauge AI's performance in strained and complex environments.
- Putting fool-proof safeguards and efficient checks to ensure that AI systems do not transgress pre-defined security protocols.

- Defining clear ethical codes and laws to direct AI integration in NC2 systems.
- Following a step-by-step approach in adoption of AI. In the initial phase, AI systems may be ordered to perform less crucial tasks and their efficacy examined. If results are encouraging, the levels may be appropriately raised and systems re-ascertained.
- Devise a hybrid approach with some sort of human control even in human out of loop configuration. However, the scope of human supervision may be more limited than human on the loop configuration.

Effective Guards Against Cyber Threats

Cyber-attacks against AI-driven NC2 systems are not a remote possibility. This threat is more pronounced in case of non-state actors who can exploit loopholes, interfere with AI algorithms and in worst case scenarios, hack complete systems. Therefore, identification evaluation, and mitigation of potential vulnerabilities within artificial intelligence systems, and development of robust protective measures to safeguard these systems from cyber-attacks is indispensable for safety and security of NC2 systems.

Conclusion

The integration of AI into NC2 systems presents both significant opportunities and associated risks. An incremental approach with gradual transition from human on the loop to human out of the loop configuration will allow humans to use AI optimally in decision making while maintaining critical human oversight. This strategy not only mitigates immediate risks but also paves the way for future advancements in AI autonomy, ensuring that NC2 systems remain robust, reliable, and secure in the face of evolving threats. The careful, balanced integration of AI into NC2 systems has the potential to enhance strategic stability and international security, provided that ethical and safety concerns are adequately addressed.

The false alarms of the Cold War era also fail to convince analysts against AI integration with NC2 systems. The 9 November 1979 false alarm was raised when a technician mistakenly inserted a training tape into the NORAD system which simulated a large-scale Soviet Nuclear Attack (Wright, 2015). The incident also raises questions about human supervision of NC2 systems. June 3, 1980, a false alarm was caused by the malfunctioning of a 46-cent computer chip (Schlosser, 2016). Again, the malfunction was easily detected by an intelligent automated system than by a human being. If Stanislov Petrov can ascertain that five incoming ballistic missiles cannot affect Soviet second-strike capability, an AI-integrated NC2 system thoroughly trained on multiple scenarios is more likely to make better decisions in stressful environments.

The future of AI in NC3 systems depends on our ability to manage the complex relationship between technology, ethics, and strategy. By fostering a comprehensive understanding of AI's capabilities and limitations, ameliorating algorithms through continuous upgradations and testing, and developing effective safeguards, and robust ethical and legal frameworks, we can ensure that AI contributes to a safer and more stable world. The integration of AI into NC2 systems is not just a technological challenge, but also a moral and strategic imperative that requires careful consideration and responsible stewardship.

References

Aksenov, P. (2013, September 26). *Stanislav Petrov: The man who may have saved the world*. BBC News. https://www.bbc.com/news/world-europe-24280831

Barnett, J. (2020, February 14). *AI needs humans 'on the loop' not 'in the loop' for nuke detection, general says*. Fedscoop. https://fedscoop.com/ai-should-have-human-on-the-loop/

China's military strategy. (2015, May 27). https://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm

Chinese thinking on AI integration and interaction with nuclear command and control, force structure, and decision-making. (2023). Europeanleadershipnetwork.org. https://europeanleadershipnetwork.org/report/chinese-thinking-on-ai-integration-/

France, United Kingdom, & United States. (2022, July). *Principles and responsible practices for nuclear-weapon states: Working paper submitted by France, the United Kingdom of Great Britain and Northern Ireland, and the United States of America. 2020 Review Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons*. https://www.un.org/sites/un2.un.org/files/npt_conf.2020_e_wp.70.pdf

Han, H. (2022). Analysis of the potential application and impact of artificial intelligence in the nuclear warfare system. *National Defence Technology, 43*(4), 80.

Luo, X. (2019). Artificial intelligence technology may increase the risk of nuclear war. *World Affairs*, *16*, 68–69.

Ma, J. (2024, May 25). *Top VC Kai-Fu Lee says his prediction that AI will displace 50% of jobs by 2027 is 'uncannily accurate.'* Fortune. https://fortune.com/2024/05/25/ai-job-displacement-forecast-50-percent-2027-kai-fu-lee-chatgpt-openai/

Nuclear false warnings and the risk of catastrophe. (n.d.). Armscontrol.org. Retrieved March 21, 2025, from https://www.armscontrol.org/act/2019-12/focus/nuclear-false-warnings-and-risk-catastrophe

Overly, S. (2016, July 21). Humans once opposed coffee and refrigeration. Here's why we often hate new stuff. *Washington Post*. https://www.washingtonpost.com/news/innovations/wp/2016/07/21/

Rautenbach, P. (2022). Artificial Intelligence and Nuclear Command, Control, & Communications: The Risks of Integration. *Forum.effectivealtruism.org*. https://forum.effectivealtruism.org/posts/BGFk3fZF36i7kpwWM/artificial-intelligence-and-nuclear-command-control-and-1

Saltini, A. (n.d.). *AI and nuclear command, control and communications: P5 perspectives*. Europeanleadershipnetwork.org. Retrieved March 21, 2025, from https://www.europeanleadershipnetwork.org/wp-content/uploads/2023/11/AVC-Final-Report_online-version.pdf

Schlosser, E. (2016, December 23). *World War Three, by Mistake*. The New Yorker. https://www.newyorker.com/news/news-desk/world-war-three-by-mistake

Stilwell, B. (2022, March 14). *Russia's "Dead Hand" Is a Soviet-Built Nuclear Doomsday Device*. Military.com. https://www.military.com/history/russias-dead-hand-soviet-built-nuclear-doomsday-device.html

Strategic Automated Command Control System [SACCS] - United States Nuclear Forces. (2025). Fas.org. https://nuke.fas.org/guide/usa/c3i/saccs.htm

U.S. Department of Defense. (2022). *2022 Nuclear Posture Review*. *Federation of American Scientists*. https://fas.org/wp-content/uploads/2023/07/2022-Nuclear-Posture-Review.pdf

Van Vliet, V. (2024, December 10). *Six change approaches (Kotter and Schlesinger)*. Toolshero. https://www.toolshero.com/change-management/six-change-approaches-kotter/

Vincent, J. (2016, March 24). *Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day*. The Verge. https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist

Wen, L., & Long, K. (2020, June 19). *How the combination of artificial intelligence and cyber will affect nuclear safety*? Military Tech Online. https://www.secrss.com/articles/20429

Wright, D. (2015, November 9). *A nuclear false alarm that looked exactly like the real thing*. The Equation. https://blog.ucsusa.org/david-wright/nuclear-false-alarm-950/

Zab, A. (2023, October 16). *How the failure to adopt the Printing Press gave Europeans a 300-year advantage over Muslims &...* Medium. https://medium.com/how-the-failure-to-adopt-the-printing-press