Argument of Fact – Cyberwarfare

Chadwick Bennett

Dept. of English, Old Dominion University

ENGL 211C, Writing, Rhetoric, and Research

Professor Lee Knight

February 17, 2026

Introduction

In its *Winning the Race: America's AI Action Plan* (2025), the White House states that "America must continue to be the dominant force in artificial intelligence to promote prosperity and protect our economic and national security." The plan emphasizes that building advanced AI infrastructure, including semiconductors and computing capacity, is essential to maintaining U.S. global leadership. As nations compete for superiority, control of AI semiconductor manufacturing has become more than an economic issue. It is considered a matter of national security and defense. This issue matters because military systems and cyber defenses may depend on which countries control advanced AI technology. If semiconductor dominance directly determines cyber superiority, then global cyber power could become concentrated in the hands of only a few nations. While U.S. investment in advanced AI infrastructure strengthens its position in AI-enabled military systems, cyberwarfare remains less dependent on computing power because it continues to rely on human creativity and input.

AI Semiconductor Supply Chain – The Semiconductor Advantage

"The TRUMP EFFECT." The White House announces how the United States will lead the AI semiconductor race. Artificial Intelligence (AI) is rapidly changing modern military systems. The country that leads or controls the AI semiconductors will have an advantage in AI-enabled military systems. According to the White House, April 14, 2025, article, "TRUMP EFFECT: NVIDIA Leads American-Made Chips Boom," (The White House, 2025).

> "For the first time ever, chipmaking giant NVIDIA will manufacture its AI supercomputers entirely in the U.S., the company announced today - part of its pledge to produce $500 billion of AI infrastructure in the U.S. over the next four years. … Earlier this year, President Trump announced a $500 billion private investment in AI infrastructure led by OpenAI, Oracle, and Softbank, while Apple announced a $500 billion investment and TSMC announced a $100 billion investment in chips manufacturing."

Park, S. (2023), explains this, stating in "Semiconductors at the intersection of geoeconomics, technonationalism, and global value chains," how semiconductors have become important tools of national power rather than just economic products. The article discusses how countries such as the United States and China use semiconductor policies to protect national security and compete for global power. The article focuses on supply chains, export controls, and government strategies in the semiconductor industry. This source supports my argument by showing that semiconductor production is directly connected to national security. It also helps explain why the United States wants to control advanced chip manufacturing and technology for global competition and AI development.

Why is it Important?

Cyberwarfare remains less dependent on computing power because it relies more on human creativity and software vulnerabilities. Advancements in AI technology are crucial to the success of combating cyberwarfare. Having AI semiconductor chips is crucial for advancing AI technology. NVIDIA is the world's largest AI semiconductor manufacturer. The White House announcement, which solidifies that NVIDIA will manufacture its entire line of supercomputer semiconductor chips in the United States, will help the United States dominate cyberwarfare.

Nature of Cyberwarfare

Cyberwarfare is a series of strategic digital cyber attacks that a nation-state (country) uses in a hostile manner to destroy, disrupt, damage, or gain control over another country's critical systems and infrastructure. It involves using human hackers, software vulnerabilities, and social engineering. AI demand is exploding due to cloud AI training farms, defense modeling, autonomous systems, cyber threat modeling, and generative AI startups. Most of the AI demand comes from the military (defense & intelligence), commercial companies (OpenAI, Google, & Meta), data centers, financial modeling, enterprise AI integration, and academia.

AI systems, especially neural networks, require **physical computation hardware** for massive matrix multiplication and parallel tensor operations at massive scales to perform:

- Matrix multiplications
- Floating-point operations
- Memory access at high bandwidth
- Parallel processing

Today, that means semiconductor-based processors such as CPUs, GPUs, TPUs, or specialized accelerators. CPUs (Central Processing Units) are for general-purpose computations, flexible but not optimized for AI-scale matrix math. They're good for orchestration and control. GPUs (Graphics Processing Units) are highly parallel processors, excellent for matrix multiplication. They're the backbone of modern AI training. TPUs (Tensor Processing Units) are specialized accelerator chips specifically designed for neural network computation to perform matrix multiplication, neural network training and inference.

Why is it Important?

AI is not software. Even in the Cloud, AI runs on massive semiconductor farms inside data centers. The **global AI race is a hardware supply chain race**. NVIDIA, as a US manufacturer, dominates the AI semiconductor market by providing these chips, and is considered the world's most valuable semiconductor brand with $187 billion in revenue and 38.8% market share. According to Muldoon et al, "At certain points in these supply chains, a small number of companies dominate the supply of particular goods and services, such as AI chips and compute capacity." (Muldoon et al., 2025, para. 4)

Chitadze, N. (2022), explains how cybersecurity strategy has become a central part of the United States national security policy. The article discusses the political and strategic parts of cyberwarfare and how governments define and respond to threats in cyberspace. The article explains why cyberwarfare isn't about technical systems, but more about policy decisions, security planning, and strategy. This source supports my argument by showing that cyberwarfare is not only about advanced computing power but also about political strategy and national security planning. It explains how cyberwar involves human input, decision-making, and policy direction more than AI-influenced military hardware advantages.

AI & Military

Waseem, et al, explains how modern warfare is changing due to advances in AI (Artificial Intelligence) and other military technologies. The article focuses on strategic competition between the United States and China. It analyzes how artificial intelligence is used to prevent another country from using a non-nuclear military war. It discusses defense planning that discourages an attack based on the pros and cons of the risk benefits. The article states that AI technologies are reshaping military capabilities and changing the balance of power in the world. This source supports my argument by showing that artificial intelligence is important in modern military systems. It helps explain how technological advancements strengthen national security and strategic competition between major powers.

Why is it Important?

According to America's Cyber Defense Agency, Cybersecurity and Infrastructure Security Agency, Ransomware is described as "a type of malware that infects computer systems, restricting users' access to the infected systems." "Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge."

In 2016, Russia used Petya, a ransomware, in 2016 that targeted Windows systems hard drives, making them inaccessible, and demanded payment in Bitcoin to decrypt them. It then used NotPetya, a similar but destructive malware to Petya, targeting Medoc, Ukraine's equivalent of Turbo Tax, to cripple Ukraine's computer systems, financial institutions, and society.

The White House described NotPetya as the "most destructive and costly cyber-attack in history" (The White House, 2018). It stated that it was deployed by the Russian military against Ukraine and that there would be consequences. Other nations, including Canada, New Zealand, Australia, and the U.K., made similar statements, all naming Russia as the culprit.

The impact from ransomware and malware attacks is estimated to be over $10 billion, with major companies publicly reporting losses, including:

- **Maersk** – approx. $250–300 million
- **Merck & Co.** – approx. $870 million
- **FedEx** (via TNT Express) – approx. $400 million

AI is transforming modern military systems, but cyberwarfare has not become fully dependent on advanced computing power. The damage caused by ransomware and destructive malware shows that human creativity and system weaknesses still play a major role in digital conflict.

Counterargument

On the other hand, some analysts, as in Iturbe et al. (2024), argue that AI-based systems may develop or be automated at a much faster pace than one requiring human input. That would favor nations with access to advanced AI semiconductor infrastructure, giving them an advantage in both offensive and defensive cyber warfare capabilities. While Iturbe, et al. (2024) asserts that AI systems can automate at a much faster pace than humans, it does not mean human intervention isn’t necessary. The bottom line is that AI systems need some human direction, decisions, and input to decide on a course of action.

Conclusion

The US leadership made AI semiconductor infrastructure and manufacturing a national priority to strengthen its military systems and national security. However, it has been demonstrated that AI-based systems or computer power alone will not dominate the AI-based warfare. Major global ransomware and malware attacks have demonstrated that human intervention or input is still required to attack the weaknesses of countries or businesses. Understanding the difference and the need to integrate AI-technology with human-driven cyberwarfare input would be the best way to strengthen a country's evolving cyberwarfare offensive and defensive strategy.

References

Chitadze, N. (2022). U.S. cybersecurity strategy as one of the main directions of national security policy of the country. *Journal in Humanities, 11*(1).

Iturbe, E., Llorente-Vazquez, O., Rego, A., Rios, E., & Toledo, N. (2024). Unleashing offensive artificial intelligence: Automated attack technique code generation. *Computers & Security, 147*, Article 104077. https://doi.org/10.1016/j.cose.2024.104077

Muldoon, J., Valdivia, A., & Badger, A. (2025). *The politics of artificial intelligence supply chains*. *AI & Society*. Advance online publication. https://doi.org/10.1007/s00146-025-02625-y

Park, S. (2023). Semiconductors at the intersection of geoeconomics, technonationalism, and global value chains. *Social Sciences*, 12(8), 466.

The White House. (2018, February 15). *Statement from the press secretary: NotPetya cyberattack* [Press release]. The White House Archives. https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/

The White House. (2025, April 14). *TRUMP EFFECT: NVIDIA leads American-made chips boom* [Blog post]. https://www.whitehouse.gov/articles/2025/04/trump-effect-nvidia-leads-american-made-chips-boom/

The White House. (2025, July 23). *Winning the race: America's AI Action Plan*. https://www.whitehouse.gov/articles/2025/07/white-house-unveils-americas-ai-action-plan

Waseem, R., & Malik, T. (2024). U.S.-China strategic competition: Conventional deterrence & the changing face of modern warfare. *The Journal of Humanities & Social Sciences*, *32*(2), 161–183.