NORTHROP GRUMMAN

Northrop Grumman Building ‘Justified Confidence’ for Integrated Artificial Intelligence Systems

AI development aligns with U.S. Department of Defense’s ethics principles
June 28, 2021 C4ISR

“Justified confidence” in artificial intelligence is more than just new buzzwords. It’s about developing AI systems that are robust, reliable and accountable, and ensuring these attributes can be verified and validated.

The National Security Commission on Artificial Intelligence’s (NSCAI) Final Report highlights emerging consensus on the principles for using AI ethically and responsibly for defense and intelligence applications.

As the report states, if AI systems do not work as designed or are unpredictable, “leaders will not adopt them, operators will not use them, Congress will not fund them, and the American people will not support them.”

That is why justified confidence is so important for AI-enabled systems.

Essential technology for national defense

AI is pivotal technology. It is already ubiquitous in our everyday lives, from streaming services to navigation apps to secure banking.

But AI is also playing a role in national defense, such as way-finding for unmanned vehicles, automated target recognition, and many other applications that prize speed, scale and efficiency. Certain functions are simply not possible using traditional computation or manual processes.

The power of AI is its ability to learn and adapt to changing situations. The battlefield is a dynamic environment and the side that adapts fastest gains the advantage.

But like with all systems, AI is vulnerable to attack and failure. To truly harness the power of AI technology, developers must align with the ethical principles adopted by the U.S. Department of Defense.

To achieve this, companies like Northrop Grumman require a cohesive policy and governance processes for AI, spanning from development to testing and operations.

An Integrated Approach For Secure and Ethical AI

No one entity has all the answers. Delivering on the promise of robust, reliable and accountable AI systems requires a team effort – industry, government and academia all have roles to play.

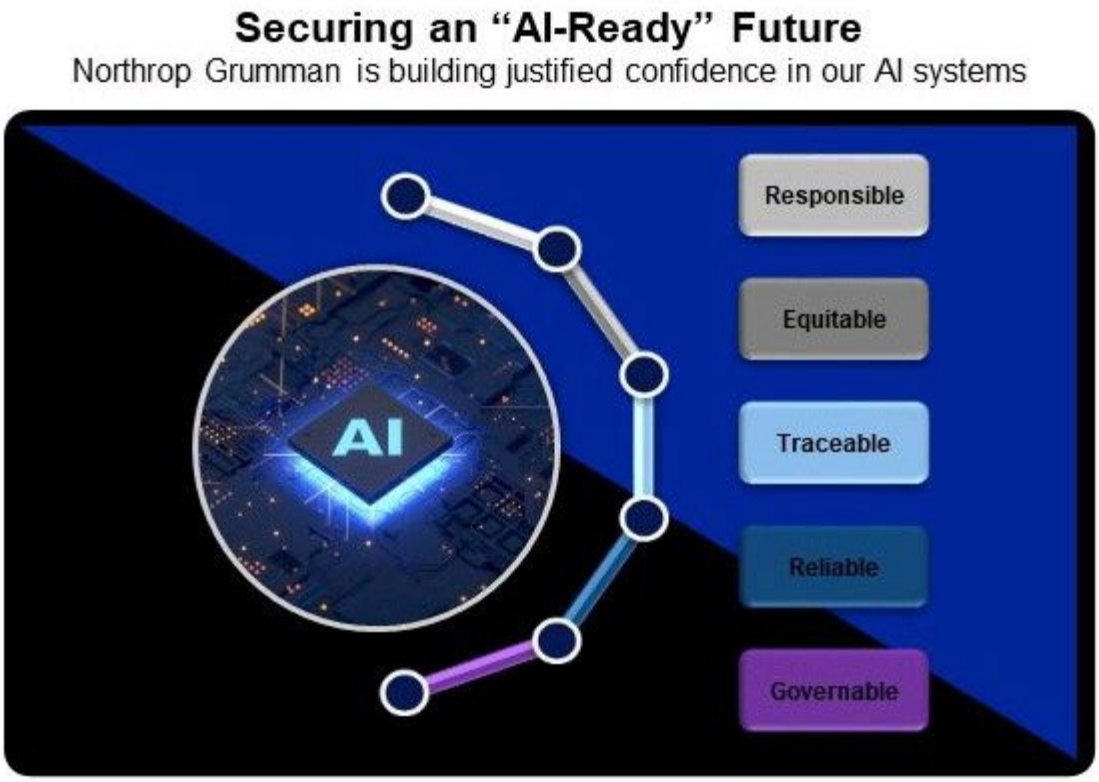
Northrop Grumman is taking a systems engineering approach to AI development and is a conduit for pulling in university research, commercial best practices and government expertise and oversight.

One of our partners is a Silicon Valley startup, Credo AI. They are sharing their governance tools as we apply comprehensive, relevant ethical AI policies to guide in own our AI development. We are also working with universities like Carnegie Mellon to develop new secure and ethical AI best practices, in addition to collaborating with leading commercial companies to advance AI technology.

Another step the company is taking is to extend our DevSecOps process to automate and document best practices in the development, testing, deployment, and monitoring of AI software systems.

Critical to success is Northrop Grumman’s AI workforce – because knowing how to develop AI technology is just one piece of the complex mosaic. Our AI engineers also understand the mission implications of the technology they develop to ensure operational effectiveness of AI systems in its intended mission space. That why we continue to invest in a mission-focused AI workforce through formal training, mentoring and apprenticeship programs.

To learn more about how Northrop Grumman is defining possible in AI, visit: https://www.northropgrumman.com/cyber/artificial-intelligence-and-machine-learning/



Aligning with the DoD’s Five Ethical Principles of AI

Northrop Grumman’s secure DevSecOps practices and mission-focused employee training helps to ensure appropriate use of judgment and care in responsible AI development.

We strive for equitable algorithms and minimize the potential for unintended bias by leveraging a diverse engineering team and testing for data bias using commercial best practices, among other monitoring techniques.

We developed tools to provide an immutable log of data provenance, ensuring traceable, transparent, and auditable development processes.

We enable reliability through an emphasis on mission understanding to develop explicit, well-defined cases in which our AI systems will operate. Leveraging best practices, our work in AI governance enables robust risk assessment, algorithmic transparency and graceful termination when required.

This integrated approach from development to operation is essential to achieving justified confidence in our AI-enabled systems.

Gabrielle Woodard
202-794-2324
gabrielle.woodard@ngc.com