



# NATO/EMERGING TECH TOPIC: AFFIRMATIVE

National Federation of State  
High School Associations



Resolved: The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization in one or more of the following areas: artificial intelligence, biotechnology, cybersecurity.

A look at possible affirmative cases, provided by Rich Edwards, Baylor University



# BAN LETHAL AUTONOMOUS WEAPONS SYSTEMS (LAWS)

- **Harm:** Violates international humanitarian law; lowers the threshold to war; escalation to nuclear war
- **Inherency:** U.S. opposition is a key obstacle to a ban
- **Solvency:** A U.S. ban provides an example that will create momentum for a ban

Human Rights Watch, Killer Robots: Military Powers Stymie Ban, Dec. 19, 2021. <https://www.hrw.org/news/2021/12/19/killer-robots-military-powers-stymie-ban>

Momentum to create new law is gathering steam with the support of a broad range and growing number of governments and political leaders, institutions, private companies, scientists, and artificial intelligence experts. Russia, the United States, India, and Israel were primarily responsible for preventing a majority of countries at the Review Conference from agreeing to open negotiations on legally binding rules on autonomous weapons systems, Human Rights Watch said.





# AI INTEROPERABILITY

- **Harm:** Failure to agree on ethical principles for the use of AI is blocking uptake. AI essential to deter war.
- **Inherency:** U.S. leadership on ethical standards for AI is lacking
- **Solvency:** Agreement on ethical principles = AI uptake in NATO

Joanna van der Merwe, (Center for European Policy Analysis), *NATO Leadership on Ethical AI is Key to Future Interoperability*, Feb. 17, 2021. <https://cepa.org/nato-leadership-on-ethical-ai-is-key-to-future-interoperability/>

The solution to the challenge that ethical AI poses for the future of interoperability within NATO is for the Alliance to establish shared transatlantic ethical principles, informed by the US DoD, the EU, and others. Establishing these principles will not only strengthen transatlantic political relations; more technically, it will allow for the establishment of standardization agreements and inform training and education initiatives of the Alliance in the future.





# DEFENCE INNOVATION ACCELERATOR FOR THE NORTH ATLANTIC (DIANA)

- **Harm:** NATO's failure to stay up to date with AI research will invite attack
- **Inherency:** U.S. has not yet signed onto DIANA
- **Solvency:** U.S. support will make the difference in making DIANA a success

Nicolas Nelson, (Center for European Policy Analysis), *Getting NATO Innovation Right*, June 18, 2021. <https://cepa.org/getting-nato-innovation-right/>

Third and finally, these new NATO bodies need to invest in or provide support to initiatives and startups without requiring external permission or consensus. At the same time, they also need a clear transition partner for promising capabilities to be handed off to (e.g. DARPA transitioning tech to the U.S. Department of Defense), which can move from development to deployment. This will enable the Alliance to more readily identify, develop, and deploy emerging and disruptive technologies. Similar efforts including the U.S. Department of Defense's DARPA and Defense Innovation Unit, CIA's In-Q-Tel, and USAF's Strategic Capabilities Office, are effective because they exist outside of traditional bureaucracies, leverage non-traditional talent strategies, and have consistent budgets.





# REMOVING GENDER BIAS FROM MACHINE LEARNING SYSTEMS

- **Harm:** Gender bias in military applications of AI promotes gender-based violence, enables deep fakes, and fails to consider the role of gender in engagement decision making.
- **Inherency:** Military applications of AI currently embed gender stereotypes.
- **Solvency:** A gender-based approach to human–machine interactions calls for a ban on military applications of AI that exacerbate gender-based harms.

**Key Source:** [https://unidir.org/sites/default/files/2021-12/UNIDIR\\_Does\\_Military\\_AI\\_Have\\_Gender.pdf](https://unidir.org/sites/default/files/2021-12/UNIDIR_Does_Military_AI_Have_Gender.pdf)



# AI AND THE SMART ELECTRICAL GRID

- **Harm:** The rate of climate change threatens human civilization and all life on Earth.
- **Inherency:** At present, the state of the U.S. electrical grid hampers the development of renewable energy.
- **Solvency:** A smart, AI-enabled electrical energy grid will speed the development of renewable energy and dramatically increase the positive impact of existing wind and solar installations.

Key Source: <https://www.intel.com/content/www/us/en/newsroom/opinion/tech-can-solve-grids-climate-change-challenge.html#gs.3b79wz>







# QUANTUM COMPUTING

- **Harm:** Advances in quantum computing will massively increase China's power and influence; quantum computers will break all existing encryption and create financial chaos.
- **Inherency:** The federal government currently undervalues quantum computing; the Quest Act was dropped from consideration.
- **Solvency:** Pass the Quest Act

**Key Source:** <https://www.theweek.co.uk/news/technology/955603/what-is-the-quantum-apocalypse>



# AUTONOMOUS SWARMING DRONES

- **Harm:** Russian aggression is ongoing; the same devastation now visited on Ukraine will spread
- **Inherency:** Biden administration defense stance is overly cautious on the use of swarming drones
- **Solvency:** Develop and deploy AI-enabled swarming drones on NATO's eastern frontier

**Key Source:** <https://www.geopoliticalmonitor.com/warfare-evolved-drone-swarms/>







# FACIAL RECOGNITION & PRIVACY PROTECTION

- **Harm:** Privacy is fundamental & is undermined at present by AI systems
- **Inherency:** Privacy protections are inadequate at present
- **Solvency:** The U.S. should follow the EU in the adoption of the General Data Privacy Regulation (GDPR)

**Key Source:** Christopher Collum, (Editor), “Owning Ourselves: Why The American Notion Of Privacy Demands A Regulatory Answer To The GDPR At The Federal Level,” *Washington University Jurisprudence Review*, 2021



# ARTIFICIAL GENERAL INTELLIGENCE & THE SINGULARITY

- **Harm:** AI systems will continue an exponential growth rate, reaching the singularity and ending human life on Earth.
- **Inherency:** Current failure to regulate AI
- **Solvency:** All necessary steps (kill switches, etc.) must be taken to maintain human control of AI.

**Key Source:** <https://interestingengineering.com/technological-singularity-an-impending-intelligence-explosion>



# BAN GERMLINE GENETIC ENGINEERING

- **Harm:** Eugenics, dehumanization, playing God with the gene pool
- **Inherency:** No current ban exists; while public funding is banned, private funding is allowed.
- **Solvency:** Ban germline genetic engineering in the U.S.

**Key Sources:** <https://time.com/5550654/crispr-gene-editing-human-embryos-ban/>

- Paschal Corby, (Prof., Bioethics, John Paul II Institute in Rome), *Hope and Despair of Bioenhancement*, 2019, 72. This denial of human distinction, and the elimination of boundaries, ultimately amounts to "the negation of man," or of what C. S. Lewis prophetically refers to as his abolition: of the human person treated as an artifact, as a mere "natural object," or "as raw material for scientific manipulation to alter at will."



# BIOLOGICAL ENHANCEMENT OF SOLDIERS

- **Harm:** Military personnel are subjected to loss of limbs, chemical contamination, etc.
- **Inherency:** Current federal restrictions on genetic engineering hamper research on protecting military personnel.
- **Solvency:** The federal government should increase funding for genetic engineering research.

## Key Source:

[https://www.army.mil/article/198685/army\\_scientists\\_regrowing\\_limbs\\_could\\_be\\_the\\_future\\_for\\_military\\_medicine](https://www.army.mil/article/198685/army_scientists_regrowing_limbs_could_be_the_future_for_military_medicine)





# DEVELOPMENT OF VACCINES

- **Harm:** Covid-19 pandemic killed millions and devastated economies; future pandemics will be worse.
- **Inherency:** The U.S. government is not prepared for the next pandemic.
- **Solvency:** Adopt and fully fund the Apollo Program for Biodefense

**Key Source:** <https://biodefensecommission.org/reports/the-apollo-program-for-biodefense-winning-the-race-against-biological-threats/>





# BAN OFFENSIVE CYBER

- **Harm:** Offensive cyber attacks risk escalation – they are seen as a prelude to attack. Attacks on missile systems are especially risky.
- **Inherency:** Both the Trump and Biden administrations are committed to offensive cyber attacks
- **Solvency:** Banning offensive cyber attacks reduces the risk of war

**Key Source:** <https://ciss.org.pk/offensive-cyber-operations-and-nuclear-weapons/>



# INCREASE DEFENSIVE CYBER

- **Harm:** Cyberattacks cause major economic harm and threaten U.S. national security
- **Inherency:** The U.S. spends much more on offensive cyber than it spends on cyber defensive
- **Solvency:** Refocus U.S. priorities on cyber defense

**Key Source:** <https://www.rand.org/pubs/perspectives/PEA512-1.html>







# DESIGNATE SPACE AS CRITICAL INFRASTRUCTURE

- **Harm:** U.S. space assets are vulnerable; cyber attacks in space threaten U.S. national security
- **Inherency:** Biden administration refuses to designate space as a critical infrastructure
- **Solvency:** Designating space as a critical infrastructure would decrease the risk of war; attackers would be on notice

**Key Source:** [https://www.insaonline.org/wp-content/uploads/2021/11/INSA\\_WP\\_Space\\_v3.pdf](https://www.insaonline.org/wp-content/uploads/2021/11/INSA_WP_Space_v3.pdf)



# CYBERSECURITY EDUCATION

- **Harm:** Cybersecurity shortage; inadequate diversity in STEM education
- **Inherency:** Federal support for STEM education & STEM diversity is inadequate
- **Solvency:** Pass the Supporting STEM Learning Opportunities Act (H.R. 6521)

Lauren Willison, (Dir., Admissions, Florida Polytechnic University), *The Case for STEM Education in Cybersecurity*, Oct. 20, 2016. Retrieved Mar. 21, 2022 from <https://insidesources.com/the-case-for-stem-education-in-cybersecurity/>

Now more than ever, our nation needs skilled professionals to protect against cyber attackers. Through innovative research, training and hands-on learning, STEM education can meet that demand by increasing the pool of skilled workers trained in cybersecurity.





# AGREEMENT ON THE CYBER ATTACK TRIGGER FOR ARTICLE V

- **Harm:** Ambiguity about what type of cyberattack might trigger Article V will lead to war with Russia.
- **Inherency:** The current declaration about cyber attacks and Article V is ambiguous
- **Solvency:** The U.S. should lead NATO in a consensus that cyber attacks should receive a cyber response, not the triggering of Article V

## Key Source:

<https://www.politico.com/news/magazine/2022/04/27/nato-credibility-cyber-defense-pledge-russia-ukraine-00027829>





# CYBER ATTRIBUTION (NAMING & SHAMING)

- **Harm:** Cyber attacks abound, risking financial and national security.
- **Inherency:** Cyber attribution is used ineffectively at present.
- **Solvency:** Cyber attribution will effectively deter if done meeting proper international evidence standards.

Kristen Eicensehr, (Prof., UCLA School of Law), “The Law and Politics of Cyberattack Attribution,” *UCLA LAW REVIEW*, July 2020, 580. Adopting an evidentiary standard of sufficient evidence to enable crosschecking would also serve the other possible purposes of attribution. Consider macro-level deterrence. For an attribution to foster macrolevel deterrence requires at least an implied threat of punishment--a responsive action such as countermeasures. For countermeasures to be viewed as lawful requires the state contemplating taking them to convince other states that it was the victim of an internationally wrongful act. Providing sufficient evidence to allow other states to verify the attribution--and thus the accused state's wrongful act--would make the threat of countermeasures more credible, increasing the deterrent effect of the attribution.





# PROTECTING ELECTIONS FROM CYBER ATTACKS

- **Harm:** Actual and potential cyber attacks undermine confidence in U.S. elections
- **Inherency:** Funding for election security is inadequate.
- **Solvency:** Proper protection of voting systems will preserve confidence in American democracy.

Jon Garon, (Dean & Professor of Law, Nova Southwestern U. College of Law), “Cyber-World War III: Origins,” *Journal of Law and Cyber Warfare*, Fall 2018, 11. The Russian attacks were also not limited to disinformation in an effort to sway or dismay voters. The Kremlin also executed direct attacks. Specifically, the New York Times reported that at least twenty-one states' "election systems were targeted by Russian hackers, according to interviews with nearly two dozen national security and state officials and election technology specialists." Some of these intrusions were aimed at voting machines, while others focused on the electronic polling records that resulted in misinformation about the polling places being delivered to voters.





# NATO/EMERGING TECH TOPIC: AFFIRMATIVE

