AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

117TH CONGRESS 2D SESSION/SENATE DOCUMENT 117–11

NATIONAL DEBATE TOPIC FOR HIGH SCHOOLS, 2022–2023

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

NATIONAL DEBATE TOPIC FOR HIGH SCHOOLS, 2022–2023
Pursuant to 44 U.S.C. Section 1333

Compiled by the Congressional Research Service
Library of Congress

U.S. Government Publishing Office
Washington, DC 2022

CHAPTER 13—PARTICULAR REPORTS AND DOCUMENTS

Sec. 1333. National high school and college debate topics

(a) The Librarian of Congress shall prepare compilations of pertinent excerpts, bibliographical references, and other appropriate materials relating to:

(1) the subject selected annually by the National University Extension Association as the national high school debate topic and

(2) the subject selected annually by the American Speech Association as the national college debate topic.

In preparing the compilations the Librarian shall include materials which in his judgment are representative of, and give equal emphasis to, the opposing points of view on the respective topics.

(b) The compilations on the high school debate topics shall be printed as Senate documents and the compilations on the college debate topics shall be printed as House of Representative documents, the cost of which shall be charged to the congressional allotment for printing and binding. Additional copies may be printed in the quantities and distributed in the manner the Joint Committee on Printing directs.

(P.L. 90–620, Oct. 22, 1968, 82 Stat. 1270)

Historical and Revision Notes
Based on 44 U.S. Code, 1964 ed., Supp. III, Sec. 170 [Sec. 276a] (Dec. 30, 1963, Pub. L. 88–246, Secs. 1, 2, 77 Stat. 802), 1964 ed., Supp. III, Sec. 170 [Sec. 276a] (Dec. 30, 1963, Pub. L. 88–246, Secs. 1, 2, 77 Stat. 802)

CONTENTS

Foreword

The 2022–2023 high school debate topic is: "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."

In compliance with 44 U.S.C., Section 1333, the Congressional Research Service (CRS) and the Law Library of the Library of Congress prepared this bibliography to assist high school debaters in researching the topic. This bibliography is intended to assist debaters in the identification of further references and resources on the subject. In selecting items for inclusion in this bibliography, the Library of Congress has sampled a wide spectrum of opinions reflected in the current literature on this topic. No preference for any policy is indicated by the selection or positioning of articles, books, or websites cited, nor is the Library's disapproval of any policy, position, or article to be inferred from its omission.

The bibliography was prepared by Audrey Crane-Hirsch, Devon Galena, and Gary Sidor of the Knowledge Services Group, CRS, Rachael Roan and Alexandra Kosmidis of the Resources, Science and Industry Division, CRS, and Anna Price of the Law Library, Library of Congress, under the direction of project team leader Caitlin Curran, with assistance from Brian Humphreys.

We wish the best to each debater as they research, prepare, and present arguments on this year's topic.

Mary B. Mazanec, Director
Congressional Research Service

NATIONAL DEBATE TOPIC FOR HIGH SCHOOLS, 2022-2023

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.

AN ANNOTATED BIBLIOGRAPHY ON THE 2022-2023 HIGH SCHOOL DEBATE TOPIC

Compiled by
Audrey Crane-Hirsch,
Devon Galena,
Gary Sidor,
Knowledge Services Group,
Congressional Research Service
and
Alexandra Kosmidis,
Rachael Roan,
Resources, Science and Industry Division
Congressional Research Service
and
Anna Price
The Law Library
Library of Congress

Under the direction of Caitlin Curran,
Knowledge Services Group,
Congressional Research Service

July 2022

Introduction

The 2022-2023 high school debate topic is: “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.” The topic is selected annually by ballot of the delegates from the National Catholic Forensic League, the National Debate Coaches Association, and the National Speech and Debate Association, all organized under the umbrella organization, the National Federation of State High School Associations.

This selective bibliography, with brief annotations, is intended to assist debaters in identifying resources and references on the national debate topic. It lists citations to articles, books, congressional publications, and websites.

Summary

The purpose of the bibliography is to provide students with a brief overview of information related to the 2022-2023 high school debate topic.

This compilation is not intended to provide complete coverage of the topic. Further research on the topic may be accomplished at high school, public, and research libraries.

In addition to the resources included in this bibliography, there are many more international organizations, U.S. government agencies, and non-governmental organizations that provide information on the debate topic and sub-topics on their websites. Debaters are encouraged to consult library resources as well as the internet for their research.

Basic Concepts and Definitions

Artificial Intelligence

Reports

Bipartisan Policy Center. *Artificial Intelligence and National Security*. Washington, DC: July 30, 2020.
Available at https://bipartisanpolicy.org/report/ai-national-security.
The Bipartisan Policy Center and Georgetown University's Center for Security and Emerging Technology consulted with Members of Congress, government officials, academics, and industry representatives about the artificial intelligence-related security challenges faced by the United States. This report seeks to explain these challenges and provide policy recommendations. One section includes specific recommendations on how the United States should work with its allies and partners.

Morgan, Forrest E., Benjamin Boudreaux, Andrew J. Lohn, Mark Ashby, Christian Curriden, Kelly Klima, and Derek Grossman. *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*. Santa Monica, CA: RAND Corporation, 2020.
Available at https://www.rand.org/pubs/research_reports/RR3139-1.html.
This report examines the benefits and risks of using artificial intelligence in military applications. It examines the extent to which the U.S. government should regulate the development of military artificial intelligence and the ethical implications of its use. Topics include military artificial intelligence in the United States, China, and Russia; public attitudes regarding military artificial intelligence; and findings and recommendations.

Websites

Association for the Advancement of Artificial Intelligence (AAAI). "A Brief History of AI."
Available at https://aitopics.org/misc/brief-history.
This timeline traces the history of artificial intelligence from the Greek myths of ancient history to the present day. It starts with a century-by-century breakdown of key events. Beginning in the 1950s, which it considers the beginning of the modern history of AI, it provides a year-by-year analysis.

Department of Energy. "DOE Explains...Artificial Intelligence."
Available at https://www.energy.gov/science/doe-explainsartificial-intelligence.
This Department of Energy webpage refers to artificial intelligence (AI) as intelligence in machines, in contrast to natural intelligence found in humans and other biological organisms." The webpage defines two key AI applications: Machine learning "involves systems that automatically learn from the data they analyze and the results they obtain to improve their ability to work with that data in the future." Deep learning "involves complex tasks" and "makes use of neural networks, which seek to build computers that operate like our brains."

Internet Encyclopedia of Philosophy. "Artificial Intelligence."
Available at https://iep.utm.edu/articicial-intelligence.
The article analyzes "intelligence" and "thought" as philosophical concepts, and summarizes philosophical arguments about "whether deeds which indicate intelligence when done by humans truly indicate it when done by machines." "Weak AI" acknowledges intelligent-acting machines; "strong AI," says such actions "can be real intelligence." "Computationalism" contends that "all thought is computation."

Biotechnology

Articles

de Lorenzo, Víctor. "15 Years of Microbial Biotechnology: The Time has Come to Think Big—and Act Soon." *Microbial Biotechnology* 15, no. 1 (Jan. 15, 2022): 240-246.
Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8719810.
The author discusses biotechnology developments over the past 15 years, from the advent of easy DNA sequencing to the potential for large-scale bioremediation of climate change. The author explains that the Earth is primarily a microbial planet and that better understanding of microorganisms is essential to avoid future threats to our environmental microbiome.

O'Brien, John T. and Cassidy Nelson. "Assessing the Risks Posed by the Convergence of Artificial Intelligence and Biotechnology." *Health Security* 18, no. 3 (May/June 2020): 219-227.
Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7310294.
As AI and biotechnology advance, there are both great opportunities and significant risks. The authors explore the criteria needed to assess risks associated with the convergence of AI and biotechnology. They evaluate the strengths and limitations of three existing risk assessment models and provide a hybrid model.

Verma, Ashish Swarup, Shishir Agrahari, Shruti Rastogi, and Anchal Singh. "Biotechnology in the Realm of History." *Journal of Pharmacy and Bioallied Sciences* 3 no. 3 (July-Sep. 2011): 321-323.
Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3178936.
The authors define biotechnology as the use of living materials biological products to create new applications for human use. The authors then discuss three phases of biotechnology's history, identifying, for example, the domestication of wild animals and the development of agriculture as aspects of "ancient biotechnology." After discussing "classic biotechnology" (1800-1940s), they highlight DNA replication and autonomous replication of synthetic genomes as highlights—to date—of "modern biotechnology."

Websites

U.S. Department of Agriculture. "Biotechnology Frequently Asked Questions." Available at https://www.usda.gov/topics/biotechnology/biotechnology-frequently-asked-questions-faqs.
This list of frequently asked questions includes a definition of agricultural biotechnology. It answers questions on how agricultural biotechnology is used, its benefits, and safety considerations. It also discusses the roles of government in agricultural biotechnology.

Cybersecurity

Articles

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. "Defining Cybersecurity." *Technology Innovation Management Review* 4(10): 13–21 (Oct. 2014). Available at http://timreview.ca/article/835.
The authors explain the importance of adopting a concise definition of cybersecurity that captures the field's multidimensionality while avoiding an overly technical view. They define cybersecurity as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." This definition, the authors argue, will encourage interdisciplinary approaches necessary to identify and battle against complex threats to cyberspace and cyberspace-enabled systems.

Reports

Carmack, Dustin and Michael Ellis. *For Cybersecurity, the Best Defense Is a Good Offense*. Washington, DC: The Heritage Foundation, 2021. Available at https://www.heritage.org/technology/report/cybersecurity-the-best-defense-good-offense.
The authors from this conservative think tank argue that traditional responses to ransomware, such as diplomatic pressure, economic sanctions, and criminal prosecutions, are insufficient. The authors write that the Fiscal Year 2019 National Defense Authorization Act affirmatively stated that offense cyber operations are "traditional military activities," allowing "deniable" cyber operations without requiring findings otherwise necessary for covert actions. The authors recommend that the United States publicly announce the threshold at which it will engage in offensive cyber operations.

Chernenko, Elana, Oleg Demidov, and Fyodor Lukyanov. *Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms*. New York: Council on Foreign Relations. Feb. 23, 2018.
Available at https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms.
The authors argue that cooperation among states is urgently needed to reduce threats from cyberattacks on infrastructure, bulk data interception, and other forms of cyber warfare. The article praises a 2016 European Parliament directive on network and information systems. By contrast, the article reports that although the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) issued a helpful set of recommendations in 2015, the group foundered in its efforts to issue a successor report in 2017.

Meltzer, Joshua P. and Cameron F. Kerry. *Cybersecurity and Digital Trade: Getting it Right*. Washington, DC: Brookings Institution, 2019.
Available at https://www.brookings.edu/research/cybersecurity-and-digital-trade-getting-it-right.
The authors discuss the significance of cyberattacks on internet-based commerce. They argue that national trade policy can and should be used to enhance private and commercial cybersecurity practices and enhance government-to-government cooperation. While restricting access to data and networks in the name of cybersecurity is a superficially appealing approach, the authors warn that doing so could harm digital trade and impair growth.

Websites

Center for Strategic & International Studies (CSIS). "Cybersecurity"
Available at https://www.csis.org/topics/cybersecurity-and-technology/cybersecurity.
This CSIS landing page links to the latest cybersecurity research from CSIS scholars. Materials include reports, commentaries, podcasts, newsletters, and blog posts. Topics include cyber warfare, encryption, military cyber capacity, hacking, and financial terrorism.

Heil, Daniel. "Cybersecurity," Hoover Institution.
Available at https://www.hoover.org/research/cybersecurity-0.
This website includes information on what cyberattacks look like, how they differ from traditional warfare, and how to defend against them. It provides links to videos that further explore the topics.

The Spectrum of Conflict

Articles

Bilal, Arsalan. "Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote." *NATO Review* (Nov. 30, 2021).
Available at https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.
This is the first article in a miniseries on "the gray zone," focusing on hybrid threats, hybrid warfare, and hybrid defense. The author explains that hybrid warfare seeks to weaken a target state's political, military, economic, social, information, and infrastructure ("PMESII") realm and weaken the state's security by undermining its legitimacy. To defend against hybrid warfare, a target state must build internal confidence and trust, especially in the way civilians think and act with the state.

Kitzen, Martijn. "Conventional And Unconventional War Are Not Opposites." War Room, U.S. Army War College (Mar. 28, 2019).
Available at https://warroom.armywarcollege.edu/articles/conventional-and-unconventional-war-are-not-opposites.
The author, an Associate Professor of War Studies at the Netherlands Defense Academy, argues that responding to complex hybrid threats requires moving beyond the dichotomy of conventional versus unconventional warfare. Kitzen contends that because Western military culture values a decisive battle in which an identifiable enemy is defeated through massive firepower and large formations, lessons about how to counter irregular forces are quickly forgotten. The author argues that Western militaries' ability to respond to contemporary hybrid threats requires learning from and building upon the lessons of counterinsurgency campaigns in Iraq and Afghanistan.

Wither, James K. "Defining Hybrid Warfare." *per Concordiam: Journal of European Security and Defense Issues* 10, no. 1 (2020): 7-9.
Available at https://www.marshallcenter.org/sites/default/files/files/2020-05/pC_V10N1_en_Wither.pdf.
The author discusses evolving understandings of the term "hybrid warfare" and explains that the phenomenon has become increasingly important since Russia's 2014 invasion and occupation of Crimea and support for rebel groups in eastern Ukraine. The author observes that the most recent definitions of "hybrid warfare" emphasize nonmilitary conflict methods, especially information and psychological warfare that targets public perceptions.

Reports

Mazarr, Michael J., Joe Cheravitch, Jeffrey W. Hornung, and Stephanie Pezard. *What Deters and Why: Applying a Framework to Assess Deterrence of Gray Zone Aggression*. Santa Monica, CA: RAND Corporation, 2021.
Available at https://www.rand.org/pubs/research_reports/RR3142.html.
The authors highlight eight core characteristics of gray zone aggressions. They identify strategies for deterring more aggressive gray zone activities and provide a framework for determining how effective these deterrent strategies are. They discuss in-depth: (1) China's gray zone aggression against the Senkaku Islands; (2) Russia's gray zone aggression against the Baltic States; and (3) North Korea's gray zone aggression against South Korea.

Morgan, Forrest E. and Raphael S. Cohen. *Military Trends and the Future of Warfare: The Changing Global Environment and Its Implications for the U.S. Air Force.* Santa Monica, CA: RAND Corporation, 2020.
Available at https://www.rand.org/content/dam/rand/pubs/research_reports/RR2800/RR2849z3/RAND_RR2849z3.pdf.
The first two chapters provide an overview of U.S. military trends. Later chapters focus on the development of asymmetric (hybrid) strategies by second-tier powers, adversaries' increased use of gray zone tactics, and how the use of artificial intelligence in military applications may change the character of war. This is one volume in RAND's The Future of Warfare series.

U.S. Library of Congress. Congressional Research Service. *Information Warfare: Issues for Congress*, by Catherine A. Theohary. R45142.
Available at https://crsreports.congress.gov/product/details?prodcode=R45142.
The report explains that "information warfare," "hybrid warfare," "active measures," and "gray zone warfare" are often (but mistakenly) used as synonyms. The report identifies information *warfare* as a form of political warfare that uses and manages information to pursue a competitive advantage through both offensive and defensive information *operations*. Information operations include cyberspace operations, psychological operations, electronic warfare, operations security, and military deception.

Websites

Atlantic Council. "Hybrid Conflict Project: Adding Color to the Gray Zone: Establishing a Strategic Framework for Hybrid Conflict."
Available at
https://www.atlanticcouncil.org/category/content-series/hybrid-warfare-project.
Forward Defense, housed within the Atlantic Council's Scowcroft Center for Strategy and Security, works to establish nonpartisan strategies to address the military/security challenges facing the United States and its allies. The Forward Defense project "Hybrid Conflict Project" investigates nontraditional and hybrid warfare threats. It provides an overview of gray zone conflict, defines key terms, and provides commentary and analysis.

Center for Strategic & International Studies (CSIS). "Gray Zone Project."
Available at https://www.csis.org/programs/gray-zone-project.
This CSIS landing page provides an overview of the gray zone phenomena and links to CSIS scholars' latest gray zone fact sheets and reports. Topics include information operations and disinformation; political and economic coercion; proxy forces, and building security partner capacity.

Overview

Global Technology Trends and the Potential Defense Applications of Artificial Intelligence, Biotechnology, and Cybersecurity

Articles

Rugge, Fabio, ed. "The Global Race for Technological Superiority." Milan: Ledzioni LediPublishing, 2019.
Available at https://www.ispionline.it/it/pubblicazione/global-race-technological-superiority-discover-security-implications-24463.
The author analyzes the effects of the global race for innovation of emerging technologies like artificial intelligence, quantum computing, and hypersonic weapons. They address the unpredictability and offer ideas to prepare for future risks.

Taeihagh, Araz, M Ramesh, and Michael Howlett. "Assessing the regulatory challenges of emerging disruptive technologies." *Regulation & Governance* 15, no. 4 (2021): 1009-1019.
Available at https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12392.
This article discusses the need for governments to consider the impact of emerging disruptive technologies, while also covering some of the regulatory challenges these technologies pose.

Yanakiev, Yantsislav, Nikolai Stoianov, Dimitar Kirkov, and Grigor Velev. "Defence strategy and new disruptive technologies nexus: implications for the military organisations." *Journal of Defence & Security Technologies* 3, issue 1, no. 2 (2020): 7-41.
Available at https://www.jdst.eu/publications/defence-strategy-and-new-disruptive-technologies-nexus-implications-military.
This article explores the role of strategy in the defense domain, emphasizing how technological innovations may influence strategy development. Using case studies of strategic documents related to defense, the authors also examine different conceptual models of defense strategy.

Books

European Parliament, Directorate-General for Parliamentary Research Services, Jacopo Bellasio, Linda Slapakova, Luke Huxtable, James Black, Theodora Ogden, and Livia Dawaele. *Shaping the 2040 Battlefield.* Brussels: European Parliament, 2021.
Available at https://op.europa.eu/en/publication-detail/-/publication/aa142c6b-518d-11ec-91ac-01aa75ed71a1.
After assessing the risks and opportunities of emerging technology alongside political, social, economic, and environmental trends, this book projects policy and innovation needs for the next 20 years of the EU's global military strategy.

Murch, Randall, Diane di Euliis. “Mapping the Cyberbiosecurity Enterprise.” Lausanne: Frontiers Media, 2019.
Available at https://www.frontiersin.org/research-topics/8353/mapping-the-cyberbiosecurity-enterprise.
This book offers several articles that discuss cyberbiosecurity through different lenses like risk analysis, national security implications, infrastructure vulnerabilities, and training for future professionals.

National Academies of Sciences, Engineering, and Medicine. *Biodefense in the Age of Synthetic Biology*. Washington, D.C: National Academies Press, 2018.
Available at https://www.ncbi.nlm.nih.gov/books/NBK535877.
While covering the benefits of synthetic biology, (the modification or creation of biological organisms), this book also covers potential threats to U.S. citizens and military personnel. It provides a way to assess those threats and mitigate the possible effects of synthetic biological attacks.

Reports

Deputy Assistant Secretary of the Army for Research and Technology. *Emerging Science and Technology Trends: A Synthesis of Leading Forecasts-5th Edition*, 2019.
Available at https://apps.dtic.mil/sti/citations/AD1078879.
This report identifies ten core trends in areas such as biomedicine, artificial intelligence, cybersecurity, and energy production. The report details current military practices and explores areas for future defense development.

Reding, D. F and J. Eaton. *Science & Technology Trends 2020-2040: Exploring the S & T Edge*. Brussels: NATO Science & Technology Organization, 2020.
Available at https://apps.dtic.mil/sti/citations/AD1131124.
This NATO report covers emerging disruptive science and technology trends forecasted to affect NATO members' military, defense, and political operations.

U.S. Department of Defense Strategic Multilayer Assessment Program. *On the Horizon: Security Challenges at the Nexus of State and Non-State Actors and Emerging/Disruptive Technologies*, 2019.
Available at https://apps.dtic.mil/sti/citations/AD1094006.
This white paper offers chapters from defense technology experts covering how technological innovation shapes approaches to national security. Topics covered include drones, cyberattacks, biosecurity, and disruptive technology.

Websites

Cybersecurity & Infrastructure Security Agency. “Cybersecurity.”
Available at https://www.cisa.gov/cybersecurity.
This portal has several pages covering different cybersecurity topics like governance, training, information sharing, and the United States’ current activities.

The U.S. Defense Industrial Base: Recent Developments in Artificial Intelligence, Biotechnology, and Cybersecurity

Reports

National Security Institute. *The U.S. Defense Industrial Base: Can it Compete in the Next Century?* 2020.
Available at https://nationalsecurity.gmu.edu/wp-content/uploads/2020/11/The-U.S.-Defense-Industrial-Base-Can-It-Compete-in-the-Next-Century-1.pdf.
The National Security Institute and geopolitical consultancy group Duco compiled this report of insights from over 100 national security experts. Key findings are about the perception of China's threat, the United States military advantage, the vulnerability of the U.S. defense industrial base, and the Department of Defense budget and processes.

U.S. Library of Congress. Congressional Research Service. *Defense Primer: U.S. Defense Industrial Base,* by Heidi M. Peters. IF10548.
Available at https://crsreports.congress.gov/product/details?prodcode=IF10548.
This report explains how the domestic and global defense industrial bases form the National Technology and Industrial Base (NTIB). It outlines critical legislation and the U.S. Department of Defense's role in assessing and utilizing NTIBcapabilities.

Websites

Brookings Institution. "The future of America's defense industrial base."
Available at
https://www.brookings.edu/events/the-future-of-americas-defense-industrial-base.
This video features the CEO of Northrop Grumman discussing innovation, threats, and the defense industry. Discussion points included the evolution of global security, the role of the United States' allies, and the future of the defense workforce.

U.S. Security Cooperation with NATO and Member Countries

Articles

Efthymiopoulos, Marios Panagiotis. "A cyber-security framework for development, defense and innovation at NATO." *Journal of Innovation and Entrepreneurship* 8, no. 1 (2019).
Available at http://dx.doi.org/10.1186/s13731-019-0105-z.
In this article, the author evaluates NATO's strategy and preparation in the face of a heightened need for cyber-defense. This examination considers global and regional needs, and the role of innovation and entrepreneurship in advancing security.

Books

Bonvillian, William B., Richard Van Atta, and Patrick Windham, eds. *The DARPA Model for Transformative Technologies: Perspectives on the U.S. Defense Advanced Research Projects Agency.* Cambridge, UK: Open Book Publishers, 2019.
Available at https://doi.org/10.11647/OBP.0184.
This book reflects on the U.S. Defense Advanced Research Projects Agency (DARPA) and its role in advancing defense and U.S. security technologies. The research featured explores the effectiveness of DARPA and the use of its model for other federal agencies and other countries.

European Parliament, Directorate-General for Parliamentary Research Services, Portesi, S., Chatzichristos, G., Drogkaris, P., et al. *Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and risks for the EU*. Brussels: European Parliamentary Research Service Scientific Foresight Unit, 2017.
Available at https://op.europa.eu/en/publication-detail/-/publication/2e35913c-1d03-11e8-ac73-01aa75ed71a1.
This study assesses EU security and defense policy and uncovers opportunities for cyber defense strategies.

Websites

NATO Cooperative Cyber Defence Centre of Excellence. "Exercises."
Available at https://ccdcoe.org/exercises.
This website describes several exercises for assessing the collaboration, training, and interoperability of cyber defense strategies in NATO nations.

The Evolving Threat Environment: Potential Adversaries' Investments in AI, Biotech, and Cyber

Russia, China, North Korea, Iran

Articles

Kim, Min-hyung, "North Korea's Cyber Capabilities and Their Implications for International Security," *Sustainability* 14, no. 3: 1744 (2022).
Available at https://www.mdpi.com/2071-1050/14/3/1744.
An article focusing on North Korea's capabilities in the "cyber-physical space" (CPS), its investments toward strengthening its cyber capabilities, and its motivations. This paper also discusses North Korea's poverty and lack of infrastructure, and examples of cyberattacks attributed to North Korea since 2014. The discussion concludes with recommendations for managing North Korea's cyber threats.

Li, Jieruo, "Artificial Intelligence Technology and China's Defense System," *Journal of Indo-Pacific Affairs* (2022).
Available at https://www.airuniversity.af.edu/JIPA/Display/Article/2980879/artificial-intelligence-technology-and-chinas-defense-system.
An in-depth discussion of China's investments in AI for military purposes, beginning with a background on China's work in this area since 2015. This article summarizes China's investments in unmanned aerial vehicles, otherwise known as drones, and their potential future military impacts.

Rim, Hyun Ji, "Emerging Technologies: New Threats and Growing Opportunities for South Korean Indo-Pacific Strategy," *Journal of Indo-Pacific Affairs* (2022).
Available at https://www.airuniversity.af.edu/JIPA/Display/Article/2979680/emerging-technologies-new-threats-and-growing-opportunities-for-south-korean-in.
This article argues that emerging technologies are at the center of geopolitical military strategies and diplomacy. It begins with a brief history of the Asia-Pacific Economic Cooperation (APEC) and then discusses actions taken by Russia and China related to AI, nuclear weapons, and space capabilities. The article concludes with strategies and opportunities, focusing on the Korean Peninsula and the United States and South Korea relationship.

Reports

Institut Français des Relations Internationales. *The Outsider: Russia in the Race for Artificial Intelligence*, by Julien Nocetti. Dec. 2020.
Available at https://www.ifri.org/sites/default/files/atoms/files/nocetti_russia_artificial_intelligence_2020.pdf.
A publication developed by an independent research center focusing on major international political and economic issues. It outlines issues related to Russia developing AI, including potential impediments and weaknesses. A chapter of this report examines the potential outcomes of the partnership between Russia and China in developing artificial intelligence.

Korea Economic Institute. *Will Artificial Intelligence Hone North Korea's Cyber "All-purpose Sword?"* by Scott W. Harold, Nathan Beauchamp-Mustafaga, Jenny Jun, Diana Myers, and Derek Grossman. Mar. 2022.
Available at https://keia.org/wp-content/uploads/2022/03/KEI_SMA_Harold-Mustafaga-Jun-Myers-Grossman.pdf.
This report focuses on North Korea and the cyber threat it presents due to its investments in AI. It includes sections on North Korea's overall policy goals and military strategy, its motivations behind investing in AI, and predictions on how the country's cyber warfare capabilities may progress. Additional research resources are extensively footnoted throughout the document.

Office of the Director of National Intelligence. *Annual Threat Assessment of the US Intelligence Community*. Apr. 9, 2021.
Available at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.
This assessment summarizes global threats to United States national security. Early chapters focus on the nations of China, Russia, North Korea, and Iran. The report also discusses transnational issues, including emerging technology (computing, biotechnology, artificial intelligence) and cybersecurity.

Stockholm International Peace Research Institute. *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, by Lora Saalman (Ed.). Oct. 2019.
Available at https://www.sipri.org/sites/default/files/2019-10/the_impact_of_artificial_intelligence_on_strategic_stability_and_nuclear_risk_volume_ii.pdf.
AI's role in national and international security risks is explained in detail in the report. Chapters cover topics such as weaponization and arms control, cyber-deterrence, machine learning, and unmanned aerial vehicles. Also included are sections dedicated to specific nations, such as Russia, China, and North Korea.

U.S. Library of Congress. Congressional Research Service. *Artificial Intelligence and National Security*, by Kelley M. Sayler. R45178. Nov. 10, 2020.
Available at https://crsreports.congress.gov/product/details?prodcode=R45178.
A comprehensive overview of various topics related to national security and AI, including lethal autonomous weapons, intelligence, surveillance, and cyberspace operations. This report also contains sections on foreign adversaries, focusing on Russia and China, with data on military investment in AI and related government initiatives.

U.S. Library of Congress. Congressional Research Service. *Emerging Military Technologies: Background and Issues for Congress*, by Kelley M. Sayler. R46458. Apr. 6, 2022.
Available at https://crsreports.congress.gov/product/details?prodcode=R46458.
This report is a primer on specific emerging military technologies in the United States, China, and Russia. Specific technologies covered include artificial intelligence, lethal autonomous weapons, hypersonic weapons, directed energy weapons, biotechnology, and quantum technology. In addition to descriptions of the different types of weapons, the report includes information regarding the relevant policies and programs of the countries analyzed. Where applicable, a brief discussion on international institutions is included.

Ukraine Conflict Effects

Articles

Erskine, Andrew “The Western Flank: The Geosecurity Periphery NATO Forgot It Had,” *Journal of Indo-Pacific Affairs* (2022).
Available at https://www.airuniversity.af.edu/JIPA/Display/Article/2964827/the-western-flank-the-geosecurity-periphery-nato-forgot-it-had.
This article gives a history of NATO's various geographical flanks, focusing on its western flank, including East Asia, China, and the Korean Peninsula. Furthermore, the article discusses the growing relationship between China and Russia, conflict in Ukraine, and how these events may affect NATO. The author argues that NATO should be reoriented to address potential threats from China and the Indo-Pacific.

Ziegler, Charles “A Crisis of Diverging Perspectives: U.S.-Russian Relations and the Security Dilemma,” *Texas National Security Review* 4, no. 1:11 (2020).
Available at http://dx.doi.org/10.26153/tsw/11708.
Although published before the 2022 Ukraine conflict, this article offers a helpful historical backdrop of diplomatic relations between the United States and Russia, covering primarily political and military competition. It also summarizes modern historical events in Ukraine from 2012-2020, and Russia’s reactions to NATO expansion before its 2022 invasion of Ukraine.

Reports

Atlantic Council. *Defending Every Inch of NATO Territory: Force Posture Options for Strengthening Deterrence in Europe*. Mar. 9, 2022.
Available at https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/us-and-nato-force-posture-options.
This report provides a brief summary of steps that NATO member states have taken to support Ukraine and deter Russian influence in Europe. Included are recommendations for maintaining nuclear deterrent capabilities and options for ensuring a unified approach by NATO allies. It also discusses cyber-attacks and enhanced AI to improve military capabilities (e.g., drones).

Canadian Global Affairs Institute. *Russian Cyber-Operations in Ukraine and the Implications for NATO*, by Alexander Salt and Maya Sobchuk. Aug. 2021.
Available at https://www.cgai.ca/russian_cyber_operations_in_ukraine_and_the_implications_for_nato.
This report focuses on Russia’s increased use of cyber-attacks since its 2014 invasion of Crimea. It urges policymakers within the United States and NATO to look at Russia's steps in the region to strengthen its cyber-capabilities. Topical sections in this document cover the history of Russian cyber-operations in Ukraine, NATO’s capabilities, and future potential conflicts between NATO nations and Russia.

Council on Foreign Relations. *Preventing a Wider European Conflict*, by Thomas Graham. Mar. 8, 2022.
Available at https://www.cfr.org/report/preventing-wider-european-conflict.
The author lists several scenarios in which Russia’s invasion of Ukraine could stretch into Europe, including cyber-attacks and disinformation campaigns. He also summarizes actions that the United States and NATO could take to prevent or mitigate conflict. The report concludes with recommendations for protecting NATO partners, such as reducing Europe’s dependence on Russian gas and increasing U.S. presence in the Indo-Pacific.

Manohar Parrikar Institute for Defense Studies and Analyses. *Russia’s AI Enabled Military Ecosystem and Its Algorithmic Warfare*, by Samur Shamra. Mar. 16, 2022.
Available at https://idsa.in/idsacomments/russias-ai-enabled-military-ecosystem-ssharma-160322.
This article discusses the weapons and military tactics that Russia used during its invasion of Ukraine. The author focuses on Russia’s commitment to using autonomous weapons, AI-based cyber-attacks, and electronic warfare. There is also a brief chronology of Russia's shift to AI from 2014 to the present.

Security Implications for the United States and NATO

Reports

Brookings Institution. *The Other 4+1: Biological, Nuclear, Climatic, Digital, and Internal Dangers*, by Michael O'Hanlon. Jan. 25, 2021.
Available at https://www.brookings.edu/research/the-other-41-biological-nuclear-climatic-digital-and-internal-dangers.
A summary of American foreign policy and national security threats from Russia, China, North Korea, Iran, and violent extremism. This article posits that threats from these actors are ever-changing, and the US government should focus its resources on specific issues, including biological weapons and nefarious use of technology. A useful discussion on cyber-attack vulnerabilities is found near the end of the report.

Carnegie Europe. *New Perspectives on Shared Security: NATO's Next 70 Years*, by Tomáš Valášek (Ed.). Nov. 28, 2019.
Available at https://carnegieeurope.eu/2019/11/28/new-perspectives-on-shared-security-nato-s-next-70-years-pub-80411.
A collection of essays discussing NATO's history, modern challenges, and future objectives. Chapters discuss topics including energy security, arms control, artificial intelligence, and the future of conflict.

Center for a New American Security. *International Stability: Risks and Confidence-Building Measures*, by Michael Horowitz and Paul Scharre. Jan. 12, 2021.
Available at https://www.cnas.org/publications/reports/ai-and-international-stability-risks-and-confidence-building-measures.
This report discusses the military use of AI and machine learning, their impacts on military practices, and their associated risks. Mainly focusing on threats, the author recommends "confidence-building measures" that nations should implement to prevent inadvertent war. The suggested measures include information-sharing, consistent policies governing military operations, and limits on military readiness and operations.

Government Accountability Office. *Long-range Emerging Threats Facing the United States as Identified by Federal Agencies*. Dec. 2018.
Available at https://www.gao.gov/assets/gao-19-204sp.pdf.
This GAO report summarizes national security threats identified by the Department of Defense, Department of State, Department of Homeland Security, and the Office of the Director of National Intelligence. Listed threats include AI, biotechnology, electronic warfare, and cyber weapons, among others. A list of publications on related national security topics is appended to the end of this document.

Government Accountability Office. *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy*. Sep. 22, 2020.
Available at https://www.gao.gov/products/gao-20-629.
This report emphasizes a need within the federal government to have clearly defined central leadership to coordinate efforts to overcome cyber-related threats. The full report describes the cyber threats facing the federal government and how they have evolved since the 1990s. Brief examples of threats to both civilian and government infrastructure are discussed.

NATO Cooperative Cyber Defence Centre of Excellence. *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, by A. Ertan, K. Floyd, P. Pernik, T. Stevens (Eds.). 2020.
Available at https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf.
An edited compilation of articles that form an exhaustive report on cyber-security issues and corresponding responses from NATO. Chapter topics include cyberspace adversaries, an analysis of new and emerging technologies, and sharing cyber threat intelligence.

Websites

North Atlantic Treaty Organization. "Deterrence and Defence."
Available at https://www.nato.int/cps/en/natohq/topics_133127.htm.
An introduction to NATO's role as a military and political alliance, with a specific focus on deterrence and defense capabilities. In addition to a summary of recent events related to NATO defense, this website summarizes some of NATO's activities on this topic, including safeguarding the security and freedom of its members, responding to a rapidly changing security environment, and maintaining NATO's military and technological edge.

Threats to Military Systems, Assets, and Networks

Reports

Office of the Director of National Intelligence. *Annual Threat Assessment of the US Intelligence Community*. Apr. 9, 2021.
Available at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf.
This assessment summarizes global threats to United States national security. Early chapters focus on the nations of China, Russia, North Korea, and Iran. The report also discusses transnational issues, including emerging technology (computing, biotechnology, artificial intelligence) and cybersecurity.

U.S. Library of Congress. Congressional Research Service. *Cybersecurity: Deterrence Policy*, by Chris Jaikaran. R47011. Jan. 18, 2022.
Available at https://crsreports.congress.gov/product/details?prodcode=R47011.
A detailed report on the theory of deterrence related to addressing cyber-attacks. Topics discussed include how the United States government has used deterrence strategies in the past, the limitations associated with a focus on deterrence, and future options for Congress. A discussion of the Cyberspace Solarium Commission's findings is included at the beginning of the report.

U.S. Library of Congress. Congressional Research Service. *Cybersecurity: Selected Cyberattacks, 2012-2021*, by Chris Jaikaran. R46974. Nov. 22, 2021.
Available at https://crsreports.congress.gov/product/details?prodcode=R46974.
This summary of cyber-attacks over the past decade provides a starting point for researchers who are new to this topic. This report includes a glossary of common cyber-attack terms, and examples of state-sponsored cyber-attacks and threats presented by private actors. Tables throughout the document summarize selected attacks, with links to external websites that provide additional details.

Threats to Critical Civilian Infrastructure

Reports

Carnegie Endowment for International Peace. *Systemic Cyber Risk: A Primer*, by David Forscey, Jon Bateman, Nick Beecroft, and Beau Woods. Mar. 7, 2022.
Available at https://carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531.
This report addresses the potential consequences of a "systemic cyber risk," which differs from more targeted attacks on individuals, businesses, and other entities. Recent examples of technological vulnerabilities are provided to help illustrate the issue. The report includes diagrams to help summarize complex ideas and technologies.

Websites

Department of Homeland Security. "Secure Cyberspace and Critical Infrastructure."
Available at https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure.
A brief explanation of threats faced by critical civil infrastructure in the United States. The webpage has expandable and collapsible menus with information about securing federal civilian networks, strengthening and securing critical infrastructure, assessing cybersecurity risks, and combating cybercrime. Includes links to related external resources on this topic.

U.S. Cybersecurity & Infrastructure Security Agency. "China Cyber Threat Overview and Advisories."
Available at https://www.cisa.gov/uscert/china.
This resource provides an overview of cybersecurity threats faced by the United States from China. Key threats listed include targeting industries and organizations, healthcare services, and the financial sector. This website also indicates that China conducts operations to steal intellectual property and other sensitive data from critical infrastructure organizations. The page includes examples of malicious cyber activity and recommendations for mitigating and detecting these threats.

U.S. Cybersecurity & Infrastructure Security Agency. "Iran Cyber Threat Overview and Advisories."
Available at https://www.cisa.gov/uscert/iran.
Includes examples of cyber-attack activities that the Iranian government has directed against the United States. Methods discussed include spearfishing, denial-of-service attacks, and theft of personally identifiable information. This website is updated regularly as more information becomes available.

U.S. Cybersecurity & Infrastructure Security Agency. "North Korea Cyber Threat Overview and Advisories."
Available at https://www.cisa.gov/uscert/northkorea.
This page summarizes cyber activity overseen by the North Korean government. It links to a report on state-sponsored cryptocurrency thefts, concluding that these government activities aim to collect intelligence, conduct attacks, and generate revenue. This site also includes information about reporting suspected malicious activity to the Cybersecurity & Infrastructure Security Agency.

U.S. Cybersecurity & Infrastructure Security Agency. “Russia Cyber Threat Overview and Advisories.”
Available at https://www.cisa.gov/uscert/russia.
A summary of Russia’s history of cyber-attacks, its reasons for conducting cyber-attacks, and key industries it targeted. According to this page, Russia has targeted entities involved with COVID-19 research, elections organizations, and critical manufacturing, among other sectors. Several of the facts on this page were obtained through joint efforts by the United States, Australia, Canada, New Zealand, and the United Kingdom.

U.S. Cybersecurity and Infrastructure Security Agency. “Critical Infrastructure Sectors.”
Available at https://www.cisa.gov/critical-infrastructure-sectors.
A brief overview of key critical infrastructure sectors. Industries discussed include the chemical sector, communications sector, and commercial facilities sector, among others. Each section includes an overview of the sector, potential threats it faces, and plans for mitigating and eliminating cyber-threats.

U.S. Defense Strategy: Strategic Competition for Technological Superiority and Innovation

Major Defense Research and Development Trends and Programs

Articles

Ely, David J. “A New Start for Technology: Mitigating the Impacts of Continuing Resolutions on Research and Development.” *Army Lawyer 2* (2021): 38-40.
Available at https://tjaglcs.army.mil/documents/35956/196606/The+Army+Lawyer+2021+Issue+2.pdf/1449139f-ff96-d4e9-8bcc-4be88dbf2b45?t=1634745755241.
This article analyzes the challenges U.S. defense agencies face when attempting to implement research and development programs. The author explains the obstacles inherent in advancing defense technologies due to lapses in authorization and appropriation laws.

Gholz, Eugene and Harvey M. Sapolsky. “The defense innovation machine: Why the U.S. will remain on the cutting edge.” *Journal of Strategic Studies* 44, no. 6 (2021): 854-872.
Available at https://doi.org/10.1080/01402390.2021.1917392.
The authors focus on the strengths of the United States' defense system. The article provides examples comparing the superiority of research and development in the United States, and the unique socio-political factors that make the country structurally and technologically resilient.

Harper, Jon. AUSA News: Pentagon R&E Chief Lays Out Plans for Technology Experimentation Campaign, *National Defense Magazine*, 2021.
Available at https://www.nationaldefensemagazine.org/articles/2021/10/12/pentagon-re-chief-lays-out-plans-for-technology-experimentation-campaign.
This article details a Department of Defense Research and Engineering Office (R&E office) initiative, scheduled for launch in 2023, regarding a "campaign of rapid joint experimentation." The R&E office is reviewing white papers to determine which will receive funding. Potential projects include "early indication and warning and enhanced communications."

Harrison, Adam, Bharat Rao, and Bala Mulloth. "Developing an Innovation-Based Ecosystem at the U.S. Department of Defense: Challenges and Opportunities." *Defense Horizons* 81 (2017): 1-15.
Available at https://ndupress.ndu.edu/Media/News/Article/1277806/developing-an-innovation-based-ecosystem-at-the-us-department-of-defense-challe.
This article explores research-based suggestions to ensure technological defense superiority for the U.S. Department of Defense. The authors note the development of an "innovation-based ecosystem" to promote unique approaches to innovation resulting in a network of innovators working towards a common goal.

Maye, Diane L. "Autarky or Interdependence: U.S. vs. European Security and Defense Industries in a Globalized Market." *Journal of Strategic Security* 10, no. 2 (2017): 33–47.
Available at https://digitalcommons.usf.edu/jss/vol10/iss2/3.
A comparison of the U.S. and European countries and their military security and defense spending. The article includes unique challenges to the United States that prevent efficient military spending and budgeting, which hinder advancement in certain defense areas.

Nunez, Krista A. "Negotiating in and around critical infrastructure vulnerabilities: Why the department of defense should use its other transaction authority in the new age of cyber attacks." *Public Contract Law Journal* 46, no. 3 (2017): 663–686.
Available at https://www.jstor.org/stable/26419546.
This article analyzes the Department of Defense's current cybersecurity programs and initiatives. The author promotes the "other transaction authority" (OTA) strategy to strengthen cybersecurity measures, particularly against other globally deemed powerful figures. The article includes examples of using the OTA for private and public sector cybersecurity initiatives.

Raska, Michael. "Strategic Competition for Emerging Military Technologies: Comparative Paths and Patterns." *Prism: a Journal of the Center for Complex Operations* 8, no. 3 (2020): 64-81.
Available at https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2053499/strategic-competition-for-emerging-military-technologies-comparative-paths-and.
An in-depth comparative framework of the United States defense system and other major defense powers. The author makes comparisons between Russia and China's technological defense advances. The article explains the advances and challenges present for the United States in relation to other powerful nations.

Williams, Edie. “Department of Defense Laboratories Recalibrating the Culture.” *Air & Space Power Journal* 35, no. 4 (2021): 23–35.
Available at https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-35_Issue-4/F-Williams.pdf.
This article emphasizes a need for the Department of Defense to focus on emerging technologies. The author explains the historical challenges and global competition the United States faces in their defense technologies, while suggesting that the DoD's research and development programs should refocus their investments into engineering and science R&D for ultimate success.

Reports

Cordesman, Anthony H. and Grace Hwang. “The Biden Transition and U.S. Competition with China and Russia: The Crisis-Driven Need to Change U.S. Strategy.” *Center for Strategic and International Studies*, 2020.
Available at https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/2020811.Burke_Chair.AHC_.GH9_.pdf.
This report focuses on the need for the United States to stay in competition with other major military powers such as China and Russia. The author emphasizes a change in strategy surrounding technology, science, budgeting, and programming. The section on “Competing in Military and National Security Spending” includes charts with an analysis of military spending of all three mentioned powers.

Daniels, Seamus P. “Getting to Less? The Innovation Superiority Strategy.” *Center for Strategic & International Studies*, 2020.
Available at https://www.csis.org/analysis/getting-less-innovation-superiority-strategy.
The author discusses a strategy; they call the “Innovation Superiority Strategy,” which emphasizes U.S. military innovation to ensure global competitiveness.

Kliman, Daniel, Ben FitzGerald, Kristine Lee, and Joshua Fitt. “Forging an Alliance Innovation Base.” *Center for a New American Security*, 2020.
Available at
https://www.cnas.org/publications/reports/forging-an-alliance-innovation-base.
The section “Evaluating America’s Current Approach” includes evaluations of the effectiveness of U.S. technology innovation programs, including selected defense programs. The report also notes alliances -- present and potential -- based on current programming and global memberships. Overall, the authors provide strengths and weaknesses present in the U.S. defense R&D programs.

Hourihan, Matt. “A Primer on Federal R&D Budget Trends.” *American Association of the Advancement of Science (AAAS)*, 2021.
Available at https://www.aaas.org/news/primer-federal-rd-budget-trends.
The author outlines how the federal government funds research and development (R&D) and explains the different types of R&D, including Office of Management and Budget definitions. The report includes historical and recent trends in non-defense and defense R&D.

Segal, Adam and Anya Schmemann. “Independent Task Force Report No. 77: Innovation and National Security: Keeping Our Edge.” *Council on Foreign Relations*, 2019.
Available at https://www.cfr.org/report/keeping-our-edge.
This report provides an analysis of current projects and programs supporting defense security in the United States. This includes research and development programs, past, current, and future that support science and technology innovation.

Tarraf, Danielle C., William Shelton, Edward Parker, Brien Alkire, Diana Gehlhaus, Justin Grana, Alexis Levedahl, Jasmin Léveillé, Jared Mondschein, James Ryseff, et al. “The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations,” *RAND Corporation*, 2019.
Available at https://www.rand.org/pubs/research_reports/RR4229.html.
This report, mandated by the 2019 National Defense Authorization Act, assesses the U.S. Department of Defense's artificial intelligence (AI) capabilities, provides the current state of AI and how it applies to DOD, and notes recommendations for DOD practices and implementation.

U.S. Department of Defense. “Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity.” Washington, DC: U.S. Department of Defense, 2019.
Available at https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/c.PDF.
This summary of the Department of Defense’s (DOD) Artificial Intelligence (AI) strategy includes the actions DOD is taking to enable AI development through the Joint Artificial Intelligence Center. The report also provides an overview of the strategic focus areas of the strategy.

U.S. Department of Defense. “Future Directions at the Intersection of Management Science and Information Science: A Workshop on the Emerging Sciences and Their Applicability to DoD R&D Management Challenges.” Arlington, VA: U.S. Department of Defense, 2018.
Available at https://basicresearch.defense.gov/Portals/61/FDW_Management%20Science%20and%20Information%20Science.pdf.
Compiled for a workshop held by the Department of Defense, this report includes an in-depth summary of research and development programming in response to emerging technologies in the sciences. Much of the focus is on cybersecurity and cyberattacks, emphasizing other competitive global powers. The report also includes spending and budget figures that support the need for greater involvement and proper financial allocation for science and technology defense research.

U.S. Department of Homeland Security. “S&T Artificial Intelligence & Machine Learning Strategic Plan.” Washington, DC: U.S. Department of Homeland Security, 2021.
Available at https://www.dhs.gov/publication/st-artificial-intelligence-and-machine-learning-strategic-plan.
This report presents three goals, 1) ensuring monetary investment in AI/ML research to remain resilient, 2) the use of AI/ML in homeland security efforts, and 3) training workers effectively in AI/ML. The report presents plans and approaches to achieve these goals while emphasizing the potential risks.

U.S. Department of Homeland Security. Science and Technology Directorate. *DHS Announces Two R&D Projects to Enhance Mobile Network Traffic Security.* Washington, DC: U.S. Department of Homeland Security, Science and Technology Directorate, 2021.
Available at https://www.dhs.gov/science-and-technology/news/2021/03/08/news-release-dhs-announces-two-rd-projects-enhance-mobile-network-traffic-security.
This Department of Homeland Security news release provides examples of two research and development awards from the Secure and Resilient Mobile Network Infrastructure program. The two projects focus on solutions to address the security of information and communications technologies.

U.S. Library of Congress. Congressional Research Service. *Defense Advanced Research Projects Agency: Overview and Issues for Congress*, by Marcy F. Gallo. R45088.
Available at https://crsreports.congress.gov/product/details?prodcode=R45088.
Defense Advanced Research Projects Agency (DARPA) is a Department of Defense agency that focuses on research and development (R&D) initiatives that contribute to scientific and technological advances. This report provides an overview of DARPA's history, role, and funding trends.

U.S. Library of Congress. Congressional Research Service. *Defense Primer: Emerging Technologies*, by Kelley M. Sayler. IF11105.
Available at https://crsreports.congress.gov/product/details?prodcode=IF11105.
The author highlights several emerging technologies that influence U.S. national security concerns, such as artificial intelligence, lethal autonomous weapons, hypersonic weapons, directed energy weapons, biotechnology, and quantum technology.

U.S. Library of Congress. Congressional Research Service. *The Global Research and Development Landscape and Implications for the Department of Defense*, by John F. Sargent Jr. and Marcy E. Gallo. R45403.
Available at https://crsreports.congress.gov/product/details?prodcode=R45403.
The authors provide an overview of the global research and development (R&D) landscape, focusing on the effects to the United States. The report provides analysis, and comparisons over time, of global, U.S., defense, and gross R&D expenditures for selected nations.

Websites

U.S. Department of Defense. "DOD Websites: Research Development."
Available at https://www.defense.gov/Resources/Military-Departments/DOD Websites/?category=Research+and+Development.
A listing of Department of Defense Websites associated with research and development programs.

U.S. Department of Defense. "DoD Cybersecurity Chart."
Available at https://dodiac.dtic.mil/dod-cybersecurity-policy-chart.
The website provides access to a downloadable chart, entitled "Cybersecurity-Related Policies and Issuances: Developed by the DoD Deputy CIO for Cybersecurity." It provides a listing of cybersecurity policies and guidance and includes source links, when publically available, authorities for the policies, and color-codes the policies by the "Office of Primary Responsibility" (OPR).

Major Legislative Initiatives

Articles

Furman, Jeffrey L. "The America COMPETES Acts: The Future of US Physical Science and Engineering Research?" *Innovation Policy and the Economy* 13, no. 1 (2013): 101–149. https://doi.org/10.1086/668241.
This article provides an overview of the impact of the America COMPETES Acts, particularly regarding defense programming and research. The author analyzes and compares spending and technology development in both defense and non-defense sectors, including related figures and tables.

Schwatze, Moshe. "Social and Economic Policy Goals and Their Impact on Defense Acquisition-A 2019 Update," *Defense Acquisition Research Journal* 26, no. 3 (July 2019): 208-229.
Available at
https://www.dau.edu/library/arj/ARJ/ARJ89/ARJ-89_19-827%20Schwarz.pdf.
An overview of defense procurement policies, programs, and laws affecting the acquisition and manufacturing of U.S. goods. Specific laws reviewed included the Defense Production Act, the Buy American Act, and The Berry Amendment.

Thomas, Will. "FY21 NDAA Enacted: Science and Technology Policy Highlights," *American Institute of Physics*, 2021.
Available at https://www.aip.org/fyi/2021/
fy21-ndaa-enacted-science-and-technology-policy-highlights.
The article provides summaries of the science and technology provisions within the National Defense Authorization Act (NDAA) for Fiscal Year 2021. The topics reviewed include, microelectronics, artificial intelligence, spectrum management, and emerging technologies.

Thornberry, William McClellan. "The National Defense Authorization Act: The Sturdy Ox of Legislation," *Harvard Journal on Legislation* 58, no. 1 (Winter 2021): 1-22.
Available at
https://harvardjol.com/wp-content/uploads/sites/17/2021/02/101_Thornberry.pdf.
The author, a former Representative of Texas's 13th congressional district, summarizes the legislative process and content generally included in the National Defense Authorization Act (NDAA). The NDAA "establishes and organizes the agencies responsible for national defense, sets policies for the department, and authorizes the appropriations of funds." The article highlights artificial intelligence as one of the funded research and development of new technologies considered in the NDAA.

Reports

U.S. Library of Congress. *The Defense Production Act of 1950: History, Authorities, and Considerations for Congress*, by Heidi M. Peters. R43767.
Available at https://crsreports.congress.gov/product/details?prodcode=R43767.
An overview of the Defense Production Act (DPA), its history, majority authorities, and considerations for Congress.

U.S. Library of Congress. *Semiconductors, CHIPS for America, and Appropriations in the U.S. Innovation and Competition Act (S. 1260)*, by John F. Sargent Jr. and Karen M. Sutter. IF12016.
Available at https://crsreports.congress.gov/product/details?prodcode=IF12016.
The authors provide an overview of provisions in the Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America, included in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (2021 NDAA, P.L. 116-283) as well as appropriations provisions included in the proposed United States Innovation and Competition Act (USICA, S. 1260). The provisions contain issues relating to the U.S. semiconductor manufacturing capabilities integral to the U.S. industrial competitiveness.

Defense Strategies of NATO and its Leading European Members

Member Country Defense Spending Trends and Pledges

Articles

Mackenzie, Christina, "Seven European Nations Have Increased Defense Budgets in One Month. Who Will Be Next?" *Breaking Defense*, Mar. 22, 2022.
Available at https://breakingdefense.com/2022/03/seven-european-nations-have-increased-defense-budgets-in-one-month-who-will-be-next.
This article tracks how some European countries have reacted to the conflict between Russia and Ukraine by increasing national defense spending. The report suggests that many other countries would follow that trend, and suggests what additional funds they might prioritize to protect their interests.

Molling, Christian and Schutz, Torben, "Unpacking Germany's Billion-Dollar Spending Question." *Defense News*, Mar. 11, 2022.
Available at https://www.defensenews.com/opinion/commentary/2022/03/11/unpacking-germanys-billion-dollar-spending-question.
This article questions whether Germany's commitment to greater spending on defense and international peacekeeping is enough for a country wishing to enhance its international presence. In addition to this, the authors claim that spending increases may not be prioritized if the government coalitions in power change.

Pancevski, Bojan. "Germany to Raise Defense Spending Above 2% of GDP in Response to Ukraine War." *The Wall Street Journal*, Feb. 27, 2022.
Available at https://www.wsj.com/articles/germany-to-raise-defense-spending-above-2-of-gdp-11645959425.
This article addresses Germany's pledge to reverse decades of more modest military spending, to address a conflict with international impact. This article displays how countries can shift priorities to enhance defense capabilities when a perceived threat is imminent or growing.

Reports

The Center for American Progress. *NATO's Financing Gap: Why NATO Should Create Its Own Bank,* by Max Bergman and Siena Cicarelli. Jan. 13, 2021.
Available at https://www.americanprogress.org/article/natos-financing-gap.
This report questions the current mechanism for member countries to fund NATO, and uses the inconsistency of defense obligations to argue for fundamental change. The report examines defense investments of countries made autonomously and through NATO.

North Atlantic Treaty Organization. Public Diplomacy Division. *Defence Expenditure of NATO Countries (2014-2021)*. 2021.
Available at https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210611-pr-2021-094-en.pdf.
This report provides data on defense spending for NATO countries going back to 2012. Data is presented in current dollars, as well as displayed as a percentage of all national spending as GDP for ally countries. The report contains data directly reported by countries to NATO, as well as from outside sources such as the Organization for Economic Cooperation and Development (OECD).

Websites

Global Change Data Lab. "Our World in Data: Military Spending."
Available at https://ourworldindata.org/military-spending.
This website offers custom interactive global and regional map and chart graphics of military spending. In many cases, it uses country military spending data back to the 19th century.

Stockholm International Peace Research Institute. "SIPRI Military Expenditure Database."
Available at https://www.sipri.org/databases/milex.
This website offers a longitudinal military spending compilation of countries around the world. A spreadsheet format allows users to manipulate and customize data for their needs. The database also contains tables that go back to 1988.

Member Country Defense Investment Priorities

Articles

Machi, Vivienne, "Next-Gen Tech Investments, Platform Upgrades Lead France's 2022 Defense Budget." *Defense News,* Sept. 22, 2021.
Available at https://www.defensenews.com/global/europe/2021/09/22/next-gen-tech-investments-platform-upgrades-lead-frances-2022-defense-budget.
This article examines how the French Armed Forces Ministry is enhancing its focus on technology-driven defense initiatives. As France's overall spending on defense has increased in recent years, advanced platforms and cyber defenses, including artificial intelligence and satellites, are being prioritized.

Matelly, Sylvie, "Defense Innovation and the Future of Transatlantic Strategic Superiority: A French Perspective." *The German Marshall Fund of the United States*, Apr. 9, 2018.
Available at https://www.gmfus.org/download/article/19173.
This article analyzes how innovation of military preparedness has advanced as rapidly as the advances to disruptive technologies. France is used as an example to illustrate how defense research and development must keep pace with emerging technologies and fronts.

Books

Pezard, Stephanie, Michael Shurkin, and David Ochmanek. *A Strong Ally Stretched Thin: An Overview of France's Defense Capabilities from a Burdensharing Perspective*, Santa Monica, CA: RAND Corporation, 2021.
Available at https://www.rand.org/pubs/research_reports/RRA231-1.html.
This publication addresses how France might contribute to short-term escalated conflict or a multi-national war. It addresses the facets that France might best be suited to support if collaboration with other nations is necessary.

Reports

Norwegian Ministries. Norwegian Government Security and Service Organisation. *National Cyber Security Strategy for Norway*. 2019.
Available at
https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf.
This report provides a comprehensive cyber security strategy for Norway. This example of a national strategy *not* from one of NATO's traditional contributors illustrates how countries are handling the defense of their digital infrastructures.

Member Country Defense-Related Investments in AI, Biotech, and Cyber

Articles

de Liedekerke, Arthur and Laudrain, Arthur, "Russia's Cyber War: What's Next and What the European Union Should Do." *Council on Foreign Relations*, Mar. 30, 2022.
Available at https://www.cfr.org/blog/russias-cyber-war-whats-next-and-what-european-union-should-do.
This article speculates threats European countries can expect from antagonists. It provides advice for European governments to be even more proactive than they have been over the past decade.

Hambling, David, "Huge U.K. Defense Spending Boost Funds Cyber Force, Space Command and AI." *Forbes*, Nov. 19, 2020.
Available at https://www.forbes.com/sites/davidhambling/2020/11/19/huge-uk-defense-spending-boost-funds-cyber-force-space-command-and-ai.
This article explains how the United Kingdom has made cybersecurity and artificial intelligence crucial components of its strategic defense strategy. The article depicts how these newer fronts are important to a comprehensive plan for national defense.

Machi, Vivienne, NATO Ups the Ante on Disruptive Tech, Artificial Intelligence." *Defense News*, Nov. 3, 2021.
Available at https://www.defensenews.com/digital-show-dailies/feindef/2021/11/03/nato-ups-the-ante-on-disruptive-tech-artificial-intelligence.
This article addresses how NATO has adapted to face artificial intelligence conflicts. The article illustrates how NATO and its member countries are shifting defense spending to new priorities.

North Atlantic Treaty Organization, "Emerging and Disruptive Technologies." Apr. 2022.
Available at https://www.nato.int/cps/en/natohq/topics_184303.html.
The article defines disruptive technologies and explains their growing use by adversaries as a type of warfare. NATO's strategy to combat these emerging fronts is expanding.

Reports

The German Marshall Fund of the United States. *NATO's Role in Global Cyber Security*, by Merle Maigre. Apr. 2022.
Available at https://www.gmfus.org/sites/default/files/2022-04/Maigre%20-%20NATO%20-%20Geopolitics%20-%20Cyber%20-%20final.pdf.
This report examines global cyber threats in today's climate. This author discusses the evolution of military conflicts and how to secure support for thwarting them.

Republic of France. General Secretariat for Defence and National Security. *Strategic Review of Cyber Defense*. Feb. 2018.
Available at
http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf.
The report published by the French government outlines the emerging demands for France to be prepared for cyber-attacks and cyber warfare. It introduces the framework for a comprehensive yet evolving cyber defense strategy for France.

Websites

Center for Strategic and International Studies, "Significant Cyber Incidents."
Available at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.
A website that tracks cyber-attacks around the world, including those that target NATO members. A list of attack originators is provided, as well as the scope and strategic target of the attack.

NATO Institutional Initiatives

Articles

Gilli, Andrea, "Preparing for 'NATO-mation': the Atlantic Alliance Toward the Age of Artificial Intelligence." *NATO Defense College*, Feb. 2019.
Available at https://www.ndc.nato.int/news/news.php?icode=1270.
This article addresses the changing landscape of international relations and defense, from the specific perspective of artificial intelligence. The article stresses the international obligation to keep up with the technologies of adversary countries.

Machi, Vivienne, "NATO Looking at Holistic Path to Cyber Defense Arsenal." *Defense News*. Dec. 14, 2021.
Available at https://www.defensenews.com/global/europe/2021/12/14/nato-looking-at-holistic-path-to-boost-cyber-defense-arsenal.
This article examines NATO's priority for bolstering cybersecurity as both an offensive and a defensive tactic when engaged in international conflict. The author discusses critical infrastructure components that must be protected against cyberattacks, as well as how weaknesses in NATO member country networks can be a threat to those countries with strong cyber defenses.

North Atlantic Treaty Organization, "Summary of the NATO Artificial Intelligence Strategy." Oct. 2021.
Available at https://www.nato.int/cps/en/natohq/official_texts_187617.htm.
An overview of NATO's strategic plan for using artificial intelligence is presented in this article. This approach seeks to harness technological advances rather than be outmatched by potential threats.

Reports

Istituto Affari Internazionali. *Cyber Defence in NATO Countries: Comparing Models*, by Alessandro Marrone and Ester Sabatino. 2021.
Available at https://www.iai.it/sites/default/files/iaip2105.pdf.
This report examines different types of cyber defense strategies and assesses how a variety of countries are addressing them. The paper assesses the collaborative NATO strategy for its organization's members, as well as autonomous efforts.

NATO Defense College. NATO 2030: New Technologies, New Conflicts, New Partnerships. Mar. 2021.
Available at https://www.ndc.nato.int/news/news.php?icode=1527.
This report argues that national defense in the traditional arenas has changed substantially and will continue to change. The report provides insight into how NATO member countries are adapting and illustrates how potential adversaries continue to come up with new fronts to agitate or disrupt operations.

Websites

North Atlantic Treaty Organization. “Cyber defence.”
Available at https://www.nato.int/cps/en/natohq/topics_78170.htm.
Provides a general overview of cyber threats and defense and tracks the evolution of NATO’s cyber defense activities.

SUBJECT BIBLIOGRAPHY

This section of the bibliography was compiled by the U.S. Government Publishing Office Library Services and Content Management.

These resources are freely available through the Catalog of U.S. Government Publications, https://catalog.gpo.gov, and/or available for purchase from the GPO Bookstore, https://bookstore.gpo.gov

"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."

Advanced computing, data science, and artificial intelligence research opportunities for energy-focused transportation science

Available at: https://purl.fdlp.gov/GPO/gpo172821

Publisher: National Renewable Energy Laboratory

Years/Pages: 2021; v, 18 pages

Print price: N/A

Agricultural biotechnology : overview, regulation, and selected policy issues

Available at: https://purl.fdlp.gov/GPO/gpo173690

Publisher: Congressional Research Service

Year/Pages: 2021-

Print price: N/A

Agricultural biotechnology : 21st century advancements and applications

Available at: https://purl.fdlp.gov/GPO/gpo184208

Publisher: U.S. Government Publishing Office

Year/Pages: 2022; v, 66 pages

Print price: N/A

Agriculture innovation and the federal biotechnology regulatory framework

Available at: https://purl.fdlp.gov/GPO/gpo174639

Publisher: U.S. Government Publishing Office

Year/Pages: 2022; iv, 70 pages

Print price: N/A

AI, UAVs, hypersonics, and autonomous systems : emerging technologies and Euro-Atlantic security : hearing before the Commission on Security and Cooperation in Europe, One Hundred Sixteenth Congress, second session, January 22, 2020

Available at: https://purl.fdlp.gov/GPO/gpo154195

Publisher: U.S. Government Publishing Office

Years/Pages: 2021; iii, 51 pages

Print price: N/A

Artificial intelligence : background, selected issues, and policy considerations

Available at: https://purl.fdlp.gov/GPO/gpo174251

Publisher: Congressional Research Service

Year: 2021-

Print price: N/A

Artificial intelligence : DOD should improve strategies, inventory process, and collaboration guidance : report to congressional committees

Available at: https://purl.fdlp.gov/GPO/gpo177875

Publisher: United States Government Accountability Office

Years/Pages: 2022; iii, 83 pages

Print price: N/A

Assessing the value of the NATO alliance

Available at: https://purl.fdlp.gov/GPO/gpo140280

Publisher: U.S. Government Publishing Office

Year/Pages: 2020; iii, 58 pages

Print price: N/A

Bank Secrecy Act/Anti-Money Laundering Examination Manual

Available at: https://purl.fdlp.gov/GPO/gpo14473

Publisher: Federal Financial Institutions Examination Council

Year/Pages: 2011-

Print price: N/A

Bio-inspired innovation and national security

Available at: https://purl.fdlp.gov/GPO/LPS63032

Publisher: National Defense University Press

Year/Pages: 2010; xxii, 348 pages

Print price: $16

Biotechnology

Available at: https://purl.fdlp.gov/GPO/gpo153404

Publisher: United States Department of Agriculture, Animal and Plant Health Inspection Service

Year/Pages: 2020; 1 page

Print price: N/A

Biotechnology Regulatory Services

Available at: https://purl.fdlp.gov/GPO/gpo175022

Publisher: Animal and Plant Health Inspection Service, U.S. Department of Agriculture

Year/Pages: 2022; 2 unnumbered pages

Print price: N/A

Civilian Cybersecurity Reserve Act

Available at: https://purl.fdlp.gov/GPO/gpo177695

Publisher: U.S. Government Publishing Office

Year/Pages: 2022; ii, 8 pages

Print price: N/A

Cracking down on ransomware : strategies for disrupting criminal hackers and building resilience against cyber threats

Available at: https://purl.fdlp.gov/GPO/gpo177695

Publisher: U.S. Government Publishing Office

Year/Pages: 2022; iii, 60 pages

Print price: N/A

Cybersecurity at NASA

Available at: https://purl.fdlp.gov/GPO/gpo152008

Publisher: U.S. Government Publishing Office

Year/Pages: 2021; iii, 74 pages

Print price: N/A

Cybersecurity : deterrence policy

Available at: https://purl.fdlp.gov/GPO/gpo18383

Publisher: Congressional Research Service

Year/Pages: 2022-

Print price: N/A

Cybersecurity for the new frontier

Available at: https://purl.fdlp.gov/GPO/gpo175926

Publisher: U.S. Government Publishing Office

Year/Pages: 2022; iii, 51 pages

Print price: N/A

Emerging technologies and their impact on national security : hearing before the Committee on Armed Services, United States Senate, One Hundred Seventeenth Congress, first session, February 23, 2021

Available at: https://purl.fdlp.gov/GPO/gpo175011

Publisher: U.S. Government Publishing Office

Years/Pages: 2022; iii, 66 pages

Print price: N/A

Exploratory Advanced Research Program : the role of artificial intelligence and machine learning in federally supported surface transportation

Available at: https://purl.fdlp.gov/GPO/gpo175364

Publisher: United States Department of Transportation, Federal Highway Administration

Years/Pages: 2021; x, 12 pages

Print price: N/A

Implementation of artificial intelligence to improve winter maintenance

Available at: https://purl.fdlp.gov/GPO/gpo174592

Publisher: United States Department of Transportation, Federal Highway Administration

Years/Pages: 2022; 4 unnumbered pages

Print price: N/A

Inter-allied naval relations and the birth of NATO

Available at: https://purl.fdlp.gov/GPO/gpo172929

Publisher: Naval History and Heritage Command

Year/Pages: 2020

Print price: N/A

NATO 2030: a celebration of origins and an eye toward the future (E3C Subcommittee----NATO Parliamentary Assembly joint hearing)

Available at: https://purl.fdlp.gov/GPO/gpo160373

Publisher: U.S. Government Publishing Office

Year/Pages: 2021; iii, 70 pages

Print price: N/A

Supply chain recovery and resiliency : small producers and local agricultural markets

Available at: https://purl.fdlp.gov/GPO/gpo174230

Publisher: U.S. Government Publishing Office

Year/Pages: 2022; iii, 53 pages

Print price: N/A

The role of allies and partners in U.S. military strategy and operations

Available at: https://purl.fdlp.gov/GPO/gpo158393

Publisher: U.S. Government Publishing Office

Year/Pages: 2021; iii, 105 pages

Print price: N/A

Understanding and mitigating Russian states-sponsored cyber threats to U.S. critical infrastructure

Available at: https://purl.fdlp.gov/GPO/gpo159432

Publisher: Cybersecurity & Infrastructure Security Agency, Department of Justice Federal Bureau of Investigation, National Security Agency

Year/Pages: 2022; 12 pages

Print price: N/A

Additional Resources to Search

https://catalog.gpo.gov

The Catalog of U.S. Government Publications (CGP) is the finding tool for information products published by all three branches of the U.S. Government. It includes descriptive information for current and historical publications as well as direct links to full-text documents, when available. The catalog also offers the option to locate a nearby Federal Depository Library that has a particular publication or that can provide expert assistance in finding and using related U.S. government information.

https://www.govinfo.gov

govinfo provides free public access to official publications from all three branches of the Federal Government. In addition to providing an advanced, metadata-powered search experience, govinfo also includes a content management system and a standards-compliant preservation repository.

○