THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

Protecting Critical and Emerging U.S. Technologies from Foreign Threats

October 2021

Overview

Given the unique opportunities and challenges posed by emerging technologies, the National Counterintelligence and Security Center (NCSC) today announced it is prioritizing its industry outreach efforts in a select few U.S. technology sectors where the stakes are potentially greatest for U.S. economic and national security. These sectors produce technologies that may determine whether America remains the world's leading superpower or is eclipsed by strategic competitors in the next few years. These sectors include, but are not limited to:

ARTIFICIAL INTELLIGENCE

BIOECONOMY

AUTONOMOUS SYSTEMS

QUANTUM

SEMICONDUCTORS

As mandated by Congress, a core NCSC mission is to conduct counterintelligence (CI) outreach to the U.S. private sector, academic and research communities, as well as other external stakeholders to arm them with information about foreign intelligence threats to their organizations and ways to mitigate risk. NCSC, a center within the Office of the Director of National Intelligence responsible for leading and supporting the CI and security activities of the U.S. Government, routinely partners with other federal agencies in conducting outreach to industry.

NCSC outreach to emerging technology sectors is designed to raise awareness of nation-state threats and help these sectors protect their human talent and cutting-edge research, while not stifling their innovation and scientific collaboration. NCSC seeks to safeguard these technological sectors and allow their growth and development.

Challenges and Threats from Strategic Competitors

U.S. leadership in emerging technology sectors faces growing challenges from strategic competitors who recognize the economic and military benefits of these technologies and have enacted comprehensive national strategies to achieve leadership in these areas.[1] According to the 2021 Annual Threat Assessment of the U.S. Intelligence Community, with a more level technology playing field anticipated in the future, new technological developments will increasingly emerge from multiple countries and with less warning. While the democratization of such technologies can be beneficial, it can also be economically, militarily, and socially destabilizing.[2] For this reason, advances in technologies such as computing, biotechnology, artificial intelligence, and manufacturing warrant extra attention to anticipate the trajectories of emerging technologies and understand their implications for security.[3]

The People's Republic of China (PRC) has a goal of achieving leadership in various emerging technology fields by 2030.[4] The PRC ranks as the primary strategic competitor to the United States because it has a well-resourced and comprehensive strategy to acquire and use technology to advance its national goals, including technology transfers and intelligence gathering through its Military-Civil Fusion Policy and a National Intelligence Law requiring all Chinese entities to share technology and information with the PRC military, intelligence, and security services.[5] Beijing is focused on technologies it deems critical to its economic and military future, including enabling technologies such as biotechnology, advanced computing, artificial intelligence, and others.[6]

To help achieve its strategic goals, the PRC employs a wide variety of legal, quasi-legal, and illegal methods to acquire technology and know-how from the United States and other nations. These methods include but are not limited to:

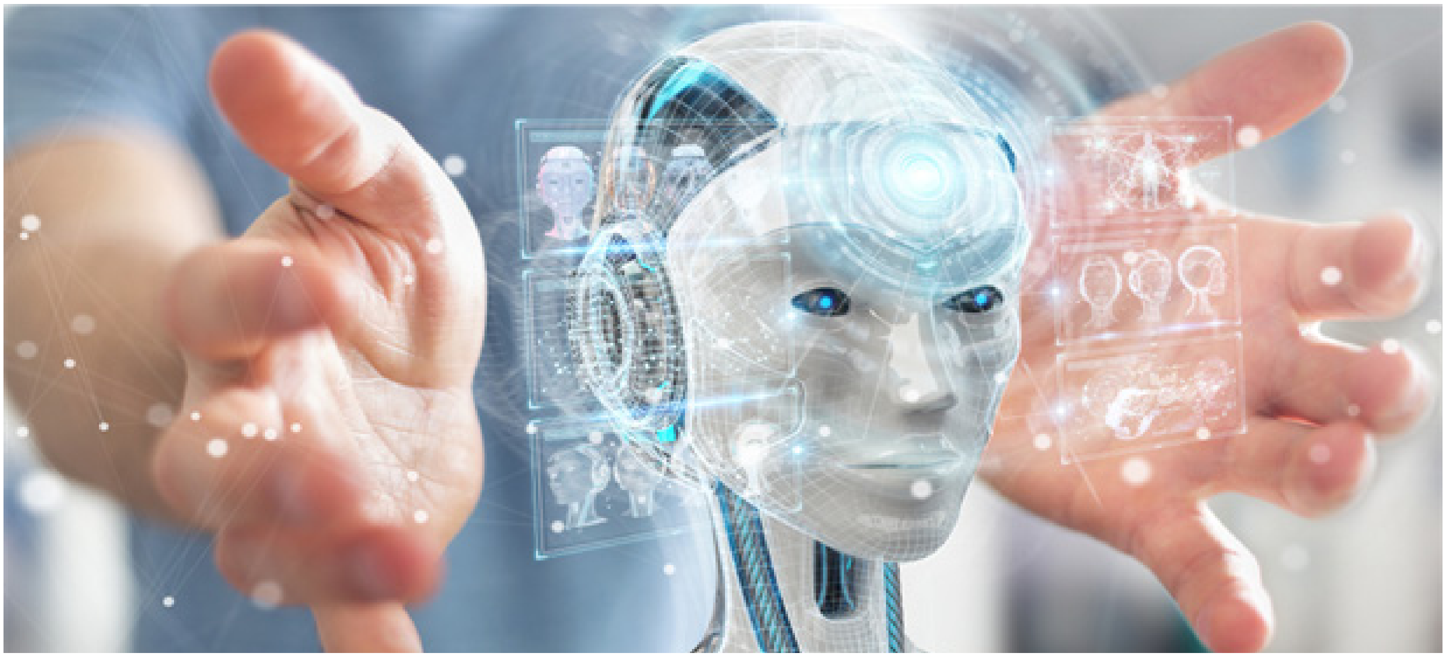
- Intelligence services
- Science and technology investments
- Academic collaboration
- Joint ventures
- Mergers and acquisitions
- Non-traditional collectors (including co-opted insiders)
- Talent recruitment programs
- Research partnerships
- Front companies
- Legal and regulatory actions

Russia views the development of advanced science and technology (S&T) as a national security priority and is targeting U.S. advances through the employment of a variety of licit and illicit technology transfer mechanisms to support national-level efforts, including its military and intelligence programs.[7] These actions include using illicit procurement networks, seeking technology transfer through joint ventures with Western companies, and requiring access to source code from technology companies seeking to sell their products in Russia.[8] Russia is increasingly looking to talent recruitment and international scientific collaborations to advance domestic research and development (R&D) efforts but resource constraints have forced it to focus indigenous R&D efforts on a few key technologies, such as military applications of Artificial Intelligence.[9]

Russia’s foreign technology acquisition toolkit includes but is not limited to:

- Intelligence services
- International scientific collaboration
- Academic collaboration
- Joint ventures and business partnerships
- Non-traditional collectors (including co-opted insiders)
- Talent recruitment
- Foreign investments
- Government-to-government agreements
- Legal and regulatory actions

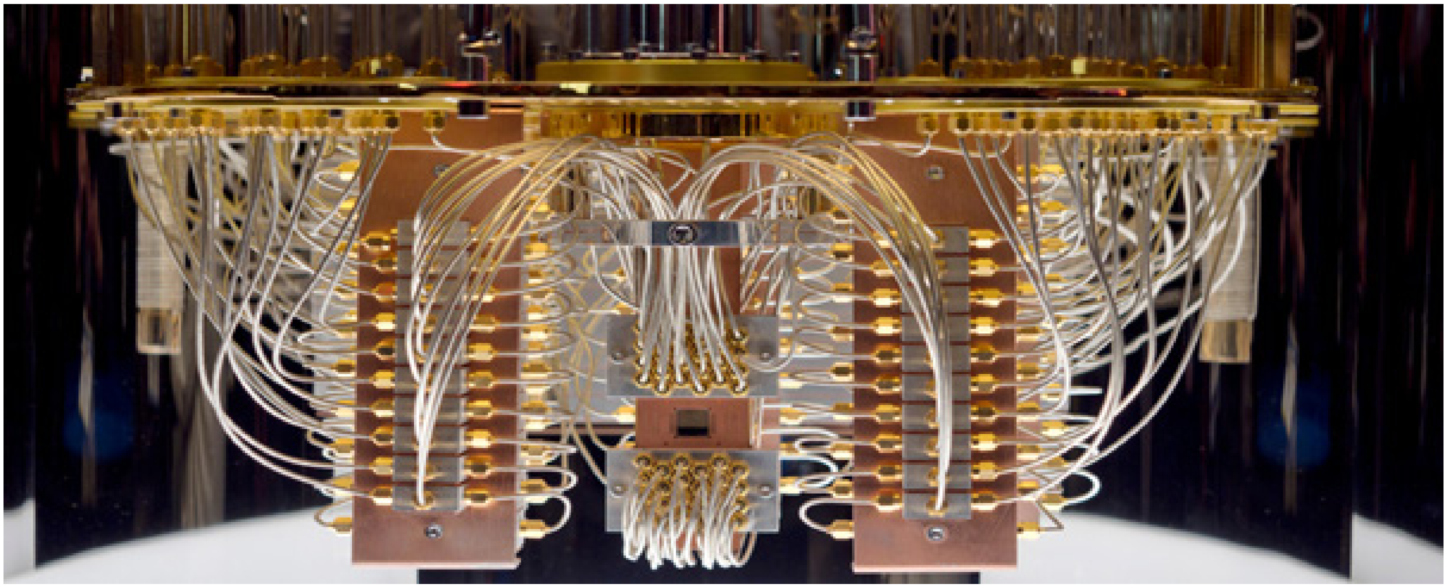
Key U.S. Emerging Technology Sectors



Artificial Intelligence (AI) is the demonstration of cognition and creative problem solving by machines rather than humans or animals, ranging from narrow AI, designed to solve specific problems, to Artificial General Intelligence, a system that in the future may match or exceed a human being's understanding and learning capacity.[10] The 2021 Final Report of the National Security Commission on Artificial Intelligence notes that AI is not one piece of hardware or software, but a constellation of technologies that requires talent, data, hardware, algorithms, applications, and integration.[11]

Benefits: AI has rapidly improved the ability of computer systems to solve problems and perform tasks that would otherwise require human intelligence and performance.[12] AI is currently embedded in devices we use and interact with daily, such as smartphones, wireless routers, and cars; and we routinely rely on AI-enriched applications, whether searching for a new restaurant, navigating traffic, or selecting a movie.[13] AI is also the quintessential "dual-use" technology. The ability of a machine to perceive, evaluate, and act more quickly and accurately than a human represents a competitive advantage in any field, civilian or military. AI technologies will be a source of enormous power for the companies and countries that harness them.[14]

Threats: AI also expands the window of vulnerability for the United States. American technological dominance is under threat by strategic competitors like the PRC, which possesses the might, talent, and ambition to potentially surpass the U.S. as the world's leader in AI in the next decade if current trends do not change.[15] AI also is deepening the threats posed by cyberattacks and disinformation campaigns that Russia, the PRC, and others are using to infiltrate our society, steal our data, and interfere in our democracy.[16] America's military rivals are also integrating AI concepts and platforms to challenge U.S. advantage.[17] Human talent, intellectual property, and R&D related to AI are targets of foreign nations seeking to enhance their own AI capabilities. Ultimately, AI is dependent on data, and the ability of adversaries to deny access to or corrupt such data poses potential vulnerabilities.



Quantum Information Science and Technology, which includes quantum computing, networking, sensing, and metrology, leverages the fundamental properties of matter to generate new information technologies. For example, quantum computers can, in principle, use the unique properties of atoms and photons to solve certain types of problems exponentially faster than a conventional computer can. Over many decades, harnessing quantum aspects of nature has produced critical technologies.

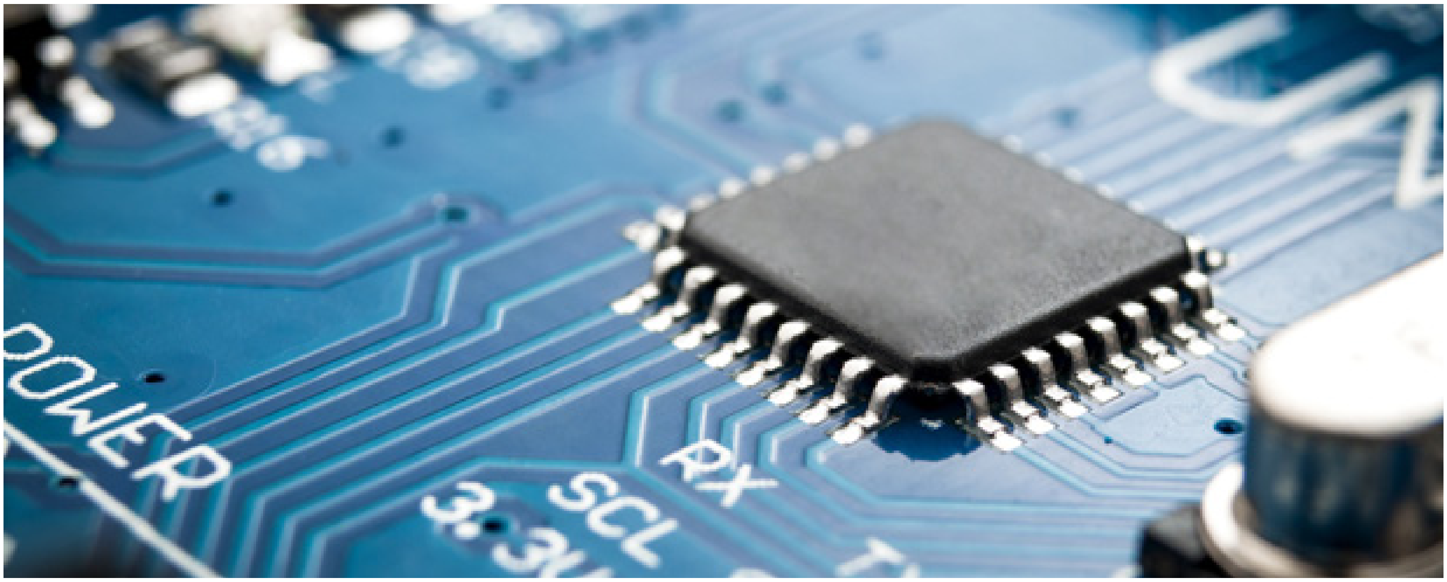
Benefits: Quantum information, science, and technology will bring new capabilities for both civilian and military purposes. Through developments in this field, the United States can improve its industrial base, create jobs, and provide economic and national security benefits.[18] Prior examples of quantum-related technologies include semiconductor microelectronics, photonics, the global positioning system, and magnetic resonance imaging, underpinning significant parts of the national economy and defense infrastructure.[19] Future scientific and technological discoveries in quantum may be even more impactful. According to the White House Office of Science and Technology Policy, U.S. Government investments in quantum and more recent industry involvement have transformed this scientific field into a nascent pillar of the American R&D enterprise.[20]

Threats: Aside from their potential benefits, quantum technologies can also pose national security challenges. With further advancements in coming years, a large-scale quantum computer could potentially allow for the decryption of most commonly used cybersecurity protocols, putting at risk the infrastructure protecting today's economic and national security communications. In short, whoever wins the race for quantum computing supremacy could potentially compromise the communications of others. Without effective mitigation, the impact of adversarial use of a quantum computer could be devastating to national security systems and the nation, especially in cases where such information needs to be protected for many decades.[21] Other quantum technologies may have future national security impacts. In the meantime, U.S. strategic competitors are recruiting America's human talent to advance their quantum programs. Some foreign nations spend substantially more than the United States on their quantum initiatives, putting them better positioned to recruit individuals.

The Bioeconomy can be defined as economic activity that is driven by research and innovation in biotechnology and is further enabled by the convergence of the life sciences and data sciences (e.g., informatics, high-performance/quantum computing, and telecommunications).

Benefits: Americans' everyday lives benefit from the U.S. bioeconomy in terms of the food they eat, the health care they receive, the quality of their environment, and the fuels, materials, and products they consume. The bioeconomy is poised to make even larger contributions in all of these sectors and expand into additional areas as well.[22] The U.S. bioeconomy provides a means of developing new and innovative products and achieving such benefits as lower carbon consumption and improved health care solutions. It also has opened new avenues for innovation, job creation, and economic growth.[23]

Threats: The powerful technologies harnessed by the bioeconomy also can lead to national security and economic vulnerabilities. For example, biotechnology can be misused to create virulent pathogens that can target our food supply or even the human population. Genomic technology used to design disease therapies tailored to an individual also can be used to identify genetic vulnerabilities in a population. Large genetic databases that allow people's ancestry to be revealed and crimes to be solved also can be misused for surveillance and societal repression.[24] During the past decade, moreover, competition in the global bioeconomy has intensified. Foreign nations have stolen critical intellectual property, research, and know-how from the U.S. bioeconomy. And, as a result of some countries' policies, an asymmetry exists in the way information is shared, whereby the ability of U.S.-based researchers to access and use such information is denied.[25] Compounding the security challenges is that many existing legal frameworks focus on protecting finished intellectual property or licensed/patented products; whereas large bodies of data – such as patient health records or genetic sequence data – represent long-term, unrealized development of products and applications.



Semiconductors such as integrated circuits are essential to modern day life and are used by the typical consumer on a daily, if not hourly, basis.[26] They permeate all aspects of our modern life, from TVs and toasters, to aircraft and satellites.

Benefits: Semiconductors enable telecommunications and grid infrastructure, run critical business and government systems, and are prevalent across a vast array of products.[27] The semiconductor-based integrated circuit is the "DNA" of technology and has transformed essentially all segments of the economy, from agriculture and transportation to healthcare, telecommunications, and the Internet. The semiconductor industry is a major engine for U.S. economic growth and job creation. Semiconductors are used in virtually every technology product and underpin state-of-the-art military systems.[28]

Threats: The global nature of the semiconductor supply chain has resulted in greater geographic concentration and interdependence, creating chokepoints that can result in interruptions and opportunities for foreign adversaries to impair U.S. access to trusted semiconductors. For instance, the United States is heavily dependent on a single company in Taiwan for producing its leading-edge chips and has significant dependence on China for mature node logic chips.[29] Since semiconductors are such key components, the fragile supply chain for semiconductors puts virtually every sector of the economy at risk of disruption.[30] In addition to impairing access, adversary exploitation of the supply chain also can prompt loss of trust in products, such as when counterfeit and compromised microchips appear in U.S. commercial and defense systems. Furthermore, adversaries can and have targeted critical technology, intellectual property, and human talent from the U.S. semiconductor industry, resulting in substantial losses. U.S. access to trusted and assured state-of-the-art semiconductor technologies is essential for the development of AI, 5G, autonomous systems, and other technologies of the future.

Autonomous Systems are not easily defined but are often described as systems that can perform tasks in a changing environment with limited human intervention or control. There are multiple degrees of autonomy. Many systems popularly known as autonomous are, in fact, semi-autonomous, rather than fully autonomous. For instance, cars with driver support systems and most unmanned aerial vehicles are semi-autonomous, while driverless cars and mobile robots in warehouses are examples of fully autonomous systems. Not all unmanned systems are autonomous.

Benefits: Autonomous systems can enhance our way of life by reducing size, costs, risk, and the need for human support, while improving productivity and safety. While autonomous vehicles receive the most attention and may have the greatest near-term economic potential, other autonomous systems and robotics have assumed key roles in tasks such as delivering goods and services, performing surgical procedures, as well as manufacturing and assembling products. Autonomous systems also have broad applications in weapons systems, including air, ground, sea surface, and undersea vehicles. In the coming years, autonomous systems are expected to become more commonly used in everyday life and capable of performing more complex tasks with reduced levels of human control.

Threats: The expansion of autonomous systems also presents new risks. Because of their dependence on software, computing, and connectivity, autonomous systems present a growing attack surface for malicious cyber actors.[31] At the same time, they can also be vulnerable to supply chain disruptions or exploitation by adversaries. Given the broad data that many of these systems collect, they are also likely to be ripe targets for foreign intelligence collection.[32] Finally, with the global competition for leadership in these sectors, particularly in autonomous vehicles, strategic competitors are already targeting U.S. technology and R&D underpinning these systems to advance their own autonomous systems.

There are many steps organizations and individuals can take to guard against nation-state threats, including the unwanted transfer of technologies, talent, and intellectual capital from the United States to strategic competitors. While the basic steps detailed below will not eliminate the threats, they can help substantially mitigate risks.

Basic Steps Organizations Can Take to Mitigate Counterintelligence Risks

- Identify, prioritize, and commit to protecting your organization's crown jewels.
- Know who you are doing business with.
  - Carefully scrutinize your suppliers, partners, and investors; understand their security practices, and set minimum standards for them.
  - Understand that all entities in the PRC, including commercial, research, and scientific, are required by law to share information with the PRC state security apparatus.
  - See additional resources at NCSC's supply chain risk management website.
- Institute a comprehensive, enterprise-wide security posture at your organization.
  - Include Acquisition, Procurement, and Human Resources in your security planning.
- Strengthen cyber security and hygiene.
  - Patch regularly, use multi-factor authentication, protect your credentials, segregate your networks, continuously monitor your systems, and maintain computer logs.
  - See additional resources at CISA's cyber essentials website.
- Implement insider threat programs.
  - See additional resources at the National Insider Threat Task Force website.
- Maintain a list of unexplained events or anomalies. Periodically review to detect patterns.
- Maintain enduring connectivity to the U.S. Government on current threat information and security best practices.
  - See resources at the FBI's counterintelligence website or the website of the Department of Defense's Center for the Development of Security Excellence.

Basic Steps Individuals Can Take to Mitigate Counterintelligence Risks

Foreign Talent Plans

- Understand the risks involved in foreign government-sponsored talent recruitment programs.
  - See FBI resources on foreign talent plans.

Personal Cyber Hygiene

- Beware of phishing / spear-phishing schemes. Never click on suspicious links or attachments.
- Use multi-factor authentication, create strong passwords (passphrases) and change often.
  - See additional resources at CISA's cyber essentials website.

Social Media

- Never accept online invitations to connect from people you don't know.
- If possible, validate online invitations through other means.
- Review social media settings to limit the amount of your information available to the public.
- Be careful what you post on social media, as it could draw attention from criminals or adversaries.
  - See additional resources from NCSC and FBI on intelligence threats and social media.

Foreign Travel

- Understand you may be targeted while traveling abroad, even to a friendly country.
- Have no expectation of privacy when traveling abroad, especially on electronic devices.
- If you can do without them, leave your electronic devices at home and take a temporary phone.
- Avoid Wi-Fi networks when abroad, if you can, as they are regularly monitored by security services.
- Never leave electronic devices unattended while abroad. A hotel safe is never "safe."
  - See NCSC awareness materials for additional resources on foreign travel and other threats.

End Notes:

[1] "National Strategy for Critical and Emerging Technologies," The White House, October 2020, pg. 1.

[2] "Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, April 2021, pg. 20.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] "National Strategy for Critical and Emerging Technologies," The White House, October 2020, pp. 1, 2.

[8] Ibid.

[9] "Annual Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, April 2021, pg. 20.

[10] "Global Trends 2040: A More Contested World," National Intelligence Council, Office of the Director of National Intelligence, March 2021, pg. 58.

[11] Final Report, National Security Commission on Artificial Intelligence, March 2021, pg. 32.

[12] Ibid, pg. 7.

[13] Ibid, pg. 33.

[14] Ibid, pg. 7.

[15] Ibid.

[16] Ibid.

[17] Ibid, pg. 2.

[18] "National Strategic Overview for Quantum Information Science," National Science & Technology Council, White House Office of Science & Technology Policy, September 2018, pg. 2.

[19] Ibid.

[20] Ibid.

[21] "Quantum Computing and Post-Quantum Cryptography," Frequently Asked Questions, National Security Agency, August 4, 2021, pg. 1.

[22] "Safeguarding the Bioeconomy," A Consensus Study Report of the National Academies of Sciences, Engineering, Medicine, National Academies Press, January 2020, pg. ix.

[23] Ibid, pg. 1

[24] Ibid, pg. ix.

[25] Ibid, pg. x.

[26] "Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth," 100-Day Reviews under Executive Order 14017, A Report by the White House, June 2021, pg. 22.

[27] Ibid, pg. 8.

[28] Ibid, pg. 22.

[29] Ibid, pp. 40, 41.

[30] Ibid, pg. 41.

[31] "National Security Implications of Leadership in Autonomous Vehicles," James Andrew Lewis, Center for Strategic and International Studies, June 28, 2021, pg. 6.

[32] Ibid, pg. 7.