2018 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Emerging Technology And National Security

Findings and recommendations to develop and deploy advanced technologies through effective partnerships that promote economic, technological, and national security competitiveness

2018 Analytic Exchange Program
July 26, 2018

2018 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Emerging Technology and National Security - Key Findings

Emerging Technology and National Security stakeholders are advocating for a more informed, deliberate, and coordinated approach to develop and deploy advanced technologies through effective partnerships

- The U.S. is at an inflection point in terms of its competitiveness and technological advancement against global competitors, friends, and foes.
- The technology sector is looking for an overarching U.S. technology strategy with specific categories for investment and development.
- The most important characteristics for emerging technology development are small, focused teams dedicated to solving specific critical issues.
- Common innovation themes identified are:
    - Think big, start small, act fast; and
    - Develop, de-risk, deploy, scale, repeat
- Modifications identified for the technology risk model include faster development and moving customers closer to the design process.
- Planning for civil liberties, privacy, and ethical impacts on national security need to be addressed in a more upfront, robust manner.
- Process and enabling activities identified include: Creating Knowledge Centers where technologists can interchange jobs over a career/product life; Revamping the security clearance process and employment practices; Modernizing acquisition programs and incentives.

2018 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Emerging Technology and National Security

Maintaining United States competitiveness in a rapidly changing technological environment

July 2018

The next decade of technological development will play a critical role in defining the national security posture and competitive position of the U.S. Emerging technologies present new opportunities, yet insert risks. Successfully managing the risks, and capitalizing on the opportunities, is not assured; competitive pressure, and the ever-increasing pace of change, compound the challenge. ***The purpose of this report is to present public and private industry stakeholders with multiple new perspectives and information on the influence of emerging technology on national security (and vice versa) while presenting recommendations to encourage and incentivize U.S. economic, technological, and military/security competitiveness well into the future***.

The Emerging Technology and National Security (ETNS) team[1] found that the U.S. must commit to a more informed, deliberate, and coordinated approach in developing and deploying emerging technologies and establishing effective partnerships. This is particularly important against a backdrop of fierce competition from state-sponsored competitors and global economic forces. Steps identified for the advancement of emerging technologies and national security include:

- Incentivizing investors and corporations to consider national security in their decision-making process while initiating partnerships/programs to foster innovation;
- Understanding the need for more partnerships and collaborative environments to share worldwide emerging technology trends, address competitive threats, share

[1] This report was written by a team of private sector and government analysts brought together by the Office of the Director of National Intelligence (ODNI) and the Department of Homeland Security (DHS).

national security concerns, and consider civil liberties, privacy, and ethical implications;

- Forming strategic public-private partnerships with the aim of allocating private capital to support national security objectives; and
- Evaluating policy and incentives to ensure the U.S. continuously maintains a competitive advantage on global economic, technological, and geopolitical stages.

Introduction & Project Approach

The Emerging Technology and National Security (ETNS) team conducted a wide-ranging, six-month study of U.S. competitiveness in key technologies (e.g. artificial intelligence, encryption, and authentication). Information for the study was drawn from a variety of sources, including a web-based survey, interviews with private sector and government stakeholders, and field research in Silicon Valley and Washington, D.C. The team met with entrepreneurs, technology companies, venture capitalists, and research firms; attended the Armed Forces Communications and Electronics Association (AFCEA) Offset Symposium; and met with leading technology companies at the April 2018 RSA Conference in San Francisco to obtain firsthand knowledge and insight from those who develop, partner, and innovate across various sectors.

> *"New technologies and novel applications of existing technologies have the potential to disrupt labor markets and alter health, energy, and transportation systems. We assess that technology developments—in the biotechnology and communications sectors, for example—are likely to outpace regulation, which could create international norms that are contrary to U.S. interests and increase the likelihood of technology surprise. Emerging technology and new applications of existing technology will also allow our adversaries to more readily develop weapon systems that can strike farther, faster, and harder and challenge the United States in all warfare domains, including space."*
>
> *Daniel R. Coats, Director of National Intelligence, February 2018*

This statement by the Director of National Intelligence (DNI) articulates some of the same challenges, and the outlook, documented by the ETNS team during the study conducted between February and June 2018.[2] For context, the ETNS team addressed emerging technologies and their applications within both the national security and private sectors.

[2] Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community, Daniel R. Coats, 13 February 2018.

Selected contextual markers for the ENTS study include:

Emerging technologies represent a wide range of evolutionary as well as disruptive innovations that have national security relevance. National security relevance can describe any technology that augments or hinders military, intelligence, or other security activities. It can also more broadly represent any innovation vis-à-vis the economic importance of a technology that can impact U.S. national security.

Adversaries, principally China, are ambitiously investing not only to close the technological gap with the United States but also to invert it. These adversaries have no pretense of limited government or prohibition of state-directed commercial activities, and they exploit their wide range of tools to quickly acquire the fast-moving technologies developing inside the adrenalized ecosystems that they project will matter most in the race for technological/economic security and superiority.

From 2015-2018, the overall pace of global economic growth has contributed to the rise in private sector technology investment and innovation.[3] Strong recent economic activity can encourage investors and provide more opportunity for exploration and risk, as the study team documented during its visits with venture capitalists in Silicon Valley. Conversely, **United States government R&D investment has been steadily declining.** This is one factor to measure and analyze how the government is responding within this global competitive space. From 1962-2017 there was a 68% decline in R&D expenditures as a percentage of the Federal Budget.[4] By 2017, between the Defense and Non-Defense sectors, R&D federal defense sector spending declined 43% from its 2007 level.[5]

---

[3] Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community, Daniel R. Coats, 13 February 2018, page 15.

[4] "R&D as Percent of the Federal Budget: FY 1962 – 2014, in outlays," American Association for the Advancement of Science https://www.aaas.org/sites/default/files/Budget.jpg ; "Historical Trends in Federal R&D," American Association for the Advancement of Science, https://www.aaas.org/page/historical-trends-federal-rd
American Association for the Advancement of Science. Beginning in FY 2017, a new official definition of R&D has been adopted by federal agencies. Late-stage development, testing, and evaluation programs, primarily within the Defense Department, are no longer counted as R&D. Source: AAAS estimates based on Budget of the U.S. Government Historical Tables.

[5] "R&D as Percent of the Federal Budget: FY 1962 – 2014, in outlays," American Association for the Advancement of Science https://www.aaas.org/sites/default/files/Budget.jpg

The Emerging Technology Landscape in the U.S.

The U.S. Government's national security approach to Emerging Technologies

> *"I beg businesspeople, when you go to Washington or you go see the mayor, don't be so parochial. Do what's right for the country. You'll be fine. If businesses are always talking about their own book, that doesn't help. If they're only there for themselves that's not good for society. If they don't get involved, it won't get better."*
>
> *Jamie Dimon, Chairman and CEO of JPMorgan Chase*

National security depends on multiple sectors working together to share technology and knowledge. The U.S. National Security Strategy (NSS) published in 2017 begins to outline key concepts to maintain the U.S.'s competitive advantage against global competitors and national security threats.

While the impact and value of the NSS remains too nascent to assess, the graph below—developed from the results of the ETNS study team survey—identifies the following as the main influencers on the development and implementation of emerging technologies:

- The U.S. government's limited incentives and declining R&D investment, along with slow acquisition timelines and speed to market opportunities
- Lack of U.S. strategic direction for key initiatives

Respondents also commented that a loss of intellectual capital and global competition influenced by state or semi-state sponsored countries influence U.S. technology development and implementation.

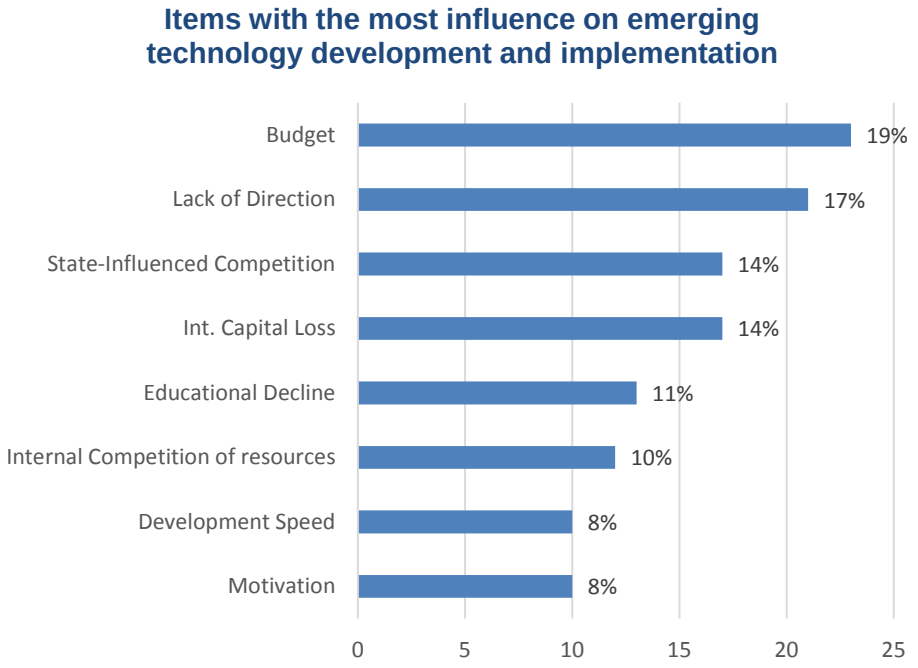

Figure 1: ETNS survey, May 2018

The team also identified disconnects in U.S. policies and roles and responsibilities within government organizations that impact technology development and knowledge transfers. For example, The Committee on Foreign Investment in the U.S. (CFIUS)[6] is one of the only organizations governing foreign investments in the U.S., particularly investments that could transfer sensitive technology to adversaries. It recently blocked the acquisition of Qualcomm by Broadcom over concerns the deal would negatively impact future U.S. technological competitiveness.

CFIUS's jurisdiction is limited and transactions that do not result in foreign controlling interest are outside their legislative purview. Joint ventures, minority investments, and purchased assets from bankruptcies which indisputably provide technology transfer are outside of the jurisdiction of the CFIUS because these transactions do not result in foreign control of an U.S. entity.

[6] The CFIUS was established by statute in the Foreign Investment and National Security Act of 2007 (FINSA) which gave an interagency working group the power to review national security implications of foreign investment in U.S. Companies or operations.

Other defensive levers the U.S. can implement to dissuade/deny technology transfer are:

- Implementing export controls;
- Evaluation procedures related to foreign students studying in U.S. schools; and
- Applying counterintelligence resources to deter technology espionage.

To counter technology transfer, a whole of government approach, along with industry participation, should identify what technologies to protect. These controls may also require collaboration with international allies, which is a long process where cooperation is not assured.[7]

The U.S. Government is attempting to share more emerging technology knowledge. For example, the National Intelligence Council (NIC) produced the report "Global Trends: The Paradox of Progress."[8] Within this public report, the NIC reexamines ideas, challenges assumptions, and forecasts future scenarios based on current trends. In reference to this report, Gregory Treverton, Chairman of the NIC, stated:

> *"…[the fact that] the National Intelligence Council regularly publishes an unclassified assessment of the world surprises some people, but our intent is to encourage open and informed discussions about future risks and opportunities. Moreover, Global Trends is unclassified because those screens of secrets that dominate our daily work are not of much help in peering out beyond a year or two. What is a help is reaching out not just to experts and government officials but also to students, women's groups, entrepreneurs, transparency advocates, and beyond."* [9]

This NIC report also makes the important point that technology is accelerating progress, but also causing discontinuity. Automation and artificial intelligence (AI) enable industries to change quicker than economies can adjust. The agile and dynamic development of

---

[7] *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation*, Defense Innovation Unit Experimental (DIUx), Michael Brown and Pavneet Singh, January 2018.

[8] The NIC serves as the U.S. Intelligence Community's center for the long-term strategic analysis, bridges the gap between intelligence and policy communities. The NIC has representation from government, academia, and the private sectors and provide expertise to the Office of the Director of National Intelligence (ODNI). See *Global Trends: The Paradox of Progress*, National Intelligence Council, Office of the Director of National Intelligence, https://www.odni.gov/files/documents/nic/GT-Full-Report.pdf

[9] *Ibid*, pg. vii.

technology and adoption could enable unprecedented advantages economically, defensively, and innovatively for countries who are involved and partner early. This highlights the criticality of the U.S. maintaining its competitive advantage, so as not to be outpaced by foreign competitors.

The U.S. Government Procurement and Acquisition Environment: The U.S. Government procurement process is arduous and lengthy. During its interviews, the study team found that this process deters technology development and innovation for national security and defense benefits. It has injected a rift between industry and government partnerships, specifically in Silicon Valley-based technology companies. The procurement process is so challenging that it is not in alignment with the speed of global technology development, especially with regards to U.S. adversaries.

However, two significant information technology procurement changes were identified in the National Defense Authorization Act for Fiscal Year 2018. One change incorporates the long-term benefit of IT investment, while another implements a Department of Defense (DoD) agency-wide audits of assets. These changes in technology, regulation, compliance, and procurement identify an interesting dynamic in the U.S. Government procurement arena. It may enhance government contractor offerings, highlight new federal departments with contracting needs, and stimulate growth. The team found that U.S. procurement processes need to be flexible and agile and have timelines in alignment with the 'digital age.'

Recently updated Other Transaction Authority (OTA) efforts within the DoD designed to execute certain prototype projects related to weapons and weapon systems can be used for basic, applied, and advanced research and prototyping in the Government's interest.[10] The OTA was recently modified to include private-public partnering on these projects and is a positive step in the direction of sharing in the early stages of technology development. The ETNS team noted that the feedback among survey and research participants about OTA was quite positive and the approach was very popular in Silicon Valley. The OTA process

[10] "Other Transactions Agreements for Prototype Projects under 10 U.S.C. 2371b," Defense Pricing/Defense Procurement and Acquisition Policy, Office of the Secretary of Defense, May 16, 2017 https://www.acq.osd.mil/dpap/cpic/cp/10USC2371bOTs.html

is substantially streamlined compared to the traditional government procurement process and allows for development to better align with the pace of technology change.

The legacy procurement processes, despite recent modifications, are structured to reduce government risk in the form of bias against contracting for technology until it reaches a more mature technical readiness level. This can impact implementation and adoption when compared to U.S. competitor technology insertion approaches.

Tax Incentives: Some current U.S. government tax benefits for companies partnering in the emerging technology space include credits for R&D expenses and advance market commitments through legally binding contracts, guaranteeing the future purchase of a product not yet developed.

However, these incentives are not sufficiently compelling for U.S. companies to work through the disjointed acquisition processes as documented in the study team's survey results. When asked to select incentives to encourage working with national security entities, respondents listed tax breaks last among six choices.

Global Approaches for Emerging Technology Development and Partnerships

The United States is currently following a different private-public partnership model than other European and Asian countries. While it is widely known and accepted that China is a state sponsor of its technology firms, different countries are implementing varying approaches to develop and exploit emerging technologies for their benefit. For example, non-adversary states, such as the United Kingdom and France are determining technologies they would like to develop nationally with other European partners and others that they will acquire through the marketplace.[11] The United Kingdom has created its own

[11] Aronsson, Lisa A., "Transatlantic Perspectives on Defense Innovation: Issues for Congress," Congressional Research Service (CRS), 24 April 2018, p. 16.

Defense Innovation Initiative to promote defense research, leverage other R&D investments, and engage with commercial innovation centers.[12]

France published its own Strategic Review on Defense and National security in October 2017. It is a broad-spectrum strategy that calls for:

- Greater military agility and responsiveness;
- More investment in space, cybersecurity, and electronic warfare capabilities; and
- Organizational and cultural change at the Ministry of Armed Forces to improve its ability to access and leverage private sector innovation.[13]

The French government also passed a "Military Programming Law" for 2019-2025 to link experts and research labs working on dual use technologies with defense contractors and armed services. They plan on increasing their R&D budget by 37% and reforming their procurement office.[14]

German advancement in innovation technologies are considered extensive, especially in the areas of autonomous vehicles, IT, and other related products and services. Of particular note is the German "Cyber Innovation Hub" which links startups mainly focused on disruptive technologies with German armed forces. The German defense strategy also emphasizes increasing R&D funding, defining national enabling technologies, and increasing cooperation with European partners.[15]

In comparison, China has targeted U.S. businesses and startups for investment and technology opportunities steadily over the last six years.[16] Chinese investment in U.S. technology companies peaked at $9.9B in 2015, as reflected in Figure 2,[17] while there was a 185% jump in Chinese investor backed deals with U.S. startups from 2013-2015. The

[12] Ibid. p. 16.
[13] Ibid. p. 18.
[14] Ibid. pp. 18-19.
[15] Ibid. p. 20.
[16] Ibid. p. 20.
[17] Bennett, Cory and Bryan Bender, "How China Acquires 'the crown jewels' of U.S. technology," *Politico*, May 22, 2018, https://www.politico.com/story/2018/05/22/china-us-tech-companies-cfius-572413

same figure reflects a decline of 12% by 2017 from the peak in 2015.[18] The jump in 2015 is reflective of the "Made in China 2025" strategy that was implemented by the Chinese government to invest in foreign technology companies. In 2016, the Obama administration took steps to block such investments leading to the decline reflected in the graph below.

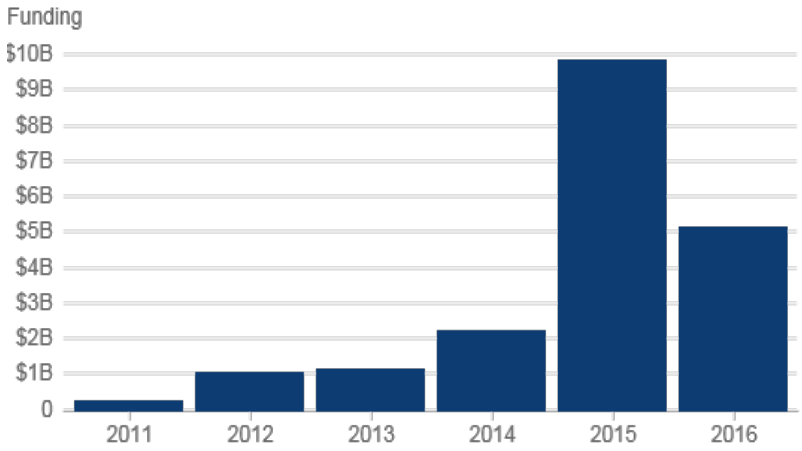

Figure 2: Money invested in U.S. technology companies from China, Hong Kong, and Taiwan, 2011-2016

The White House recently released a fact sheet detailing ideas to confront China's trade policies, which outlines the following two main trade issues the U.S. government is combating: 1) trade practices that impact fair and reciprocal trade, and 2) actively seeking to obtain technology from U.S. companies and undermine American innovation and creativity.[19]

Such competitors, using their national resources and state-sponsored support, often disguised as a commercial venture or shielded by a broker, are able to offer technology company owners values well above market levels at early stages of development. Those receiving the offers are often unwitting of the ultimate purchaser and their intentions. Using this approach, competitors are investing in sources to advance both their short and long

[18] Aronsson, Lisa A., "Transatlantic Perspectives on Defense Innovation: Issues for Congress," Congressional Research Service (CRS), 24 April 2018, p. 20.
[19] White House Fact Sheet, "President Donald J. Trump is Confronting China's Unfair Trade Policies", https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-confronting-chinas-unfair-trade-policies/, 29 May 2018.

term technology goals while staying apprised of the next generation of innovation in specific markets/regions.

Investment by China creates a national security and innovation dilemma for U.S. companies and a paradox for the Chinese. The study team found that U.S. entrepreneurs and developers need capital investment, but they may/may not have concerns about accepting foreign funding. The study team identified numerous examples of the dilemmas companies are facing: do they accept foreign funds for their projects and risk the national security (and economic) impacts on the U.S. and their potential long-term way of life, or do they have patriotic, entrenched feelings to protect national interests at the expense of an infusion of capital and the potential for more? The study team's survey identified that recognition for contributing to U.S. national security only received 14% of the responses, indicating it was not a high priority to those who responded. The decision making process investors are now faced with in a more global economy can be summarized as "Every investment comes with a risk of some loss of intellectual property or foreign influence and control."[20]

The Chinese deploy various means to acquire American technology including using bankruptcy courts or foreign venture capital companies that help fund startup firms. China has comprehensive strategies managed at the state level that synchronize foreign direct investment and direct industrial espionage across five-year cycles to dominate key technology verticals. For example, China's Belt and Road Initiative, considered to be the world's largest ever infrastructure project, is intended to provide it access and entry into more than half of the world's population and up to 40% of global GDP. Proposed by Chinese President Xi Jinping in 2013, the effort will deepen connectivity and cooperation between China and Eurasia, expand China's role in global affairs, and coordinate its manufacturing capacity with other countries. The project will also provide China and its state-backed companies with unfettered access to technology hubs and streamlined regulatory and banking constructs that will enable the quick identification and acquisition of breakthrough technologies. Furthermore, Beijing has made AI, quantum computing, and other

[20] Bennett, Cory and Bryan Bender, "How China Acquires 'the crown jewels' of U.S. technology," Politico, May 22, 2018, https://www.politico.com/story/2018/05/22/china-us-tech-companies-cfius-572413

technologies a national priority, pouring billions into R&D and human capital development.[21] The Chinese government is aggressively recruiting top talent and supports scholarship opportunities for its most promising Science, Technology, Engineering, and Mathematics (STEM) students.

An example of the conflict between national security and technology development is the recent activity of the U.S. towards the Chinese company, ZTE.[22] While it still remains undecided whether ZTE will be able to participate in the U.S. marketplace due to sanctions and national security concerns, it does highlight the dilemma within the U.S. on foreign investment and technology advancements on a global scale and specifically the Chinese approach to technology acquisition and the U.S. position reflected in the Fact Sheet on China.[23]

These varying approaches demonstrate the paradox of different policies and the societal norms associated with free markets and state-sponsored strategies in comparison to the U.S. approach that is more diversified and de-centralized. With no pretense of limited government or prohibition of state-directed commercial activities, adversaries take full advantage of their position to quickly acquire the emerging technologies that they judge critical for technological/security superiority.

[21] Elsa Kania, Genius Machines: The Next Decade of Artificial Intelligence, Wednesday, March 7, 2018.
[22] ZTE was sanctioned by the U.S. government in December 2017, only to have those restraints potentially proposed for modification in May 2018 and in June, the U.S. Senate moved to block the administration's proposal and keep the sanctions. There was no further update by the submission date of 22 July 2018.
[23] White House Fact Sheet, "President Donald J. Trump is Confronting China's Unfair Trade Policies", https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-confronting-chinas-unfair-trade-policies/, 29 May 2018.

The Critical Role of U.S. Public-Private Partnerships in Emerging Technology

The project team conducted a survey on a variety of issues for stakeholders in the emerging technology sector. One question identified important characteristics, such as small focused teams, as most critical for establishing effective public/private partnerships.

*"**Small, focused teams** dedicated to critical issues," along with "**single focused initiatives** with a specific problem to solve," were the most important characteristics to the survey respondents. The third highest response was focused on the ability to "**job share and transition between government and industry/academia.**"*

ETNS Survey May 2018

Survey respondents indicated that creating and implementing more technology grant programs designed to share initial investment/startup costs, changing government procurement and acquisition practices, and expanding civic and educational partnerships to encourage science, math, and technology participation across the U.S. were the highest ranked incentives among the respondents to encourage working with national security entities (Figure 3). The top three areas may reflect where future time, process changes, and investments need to be made to maximize the value and outcomes of public-private partnership initiatives and resource investments in the emerging technology sector.

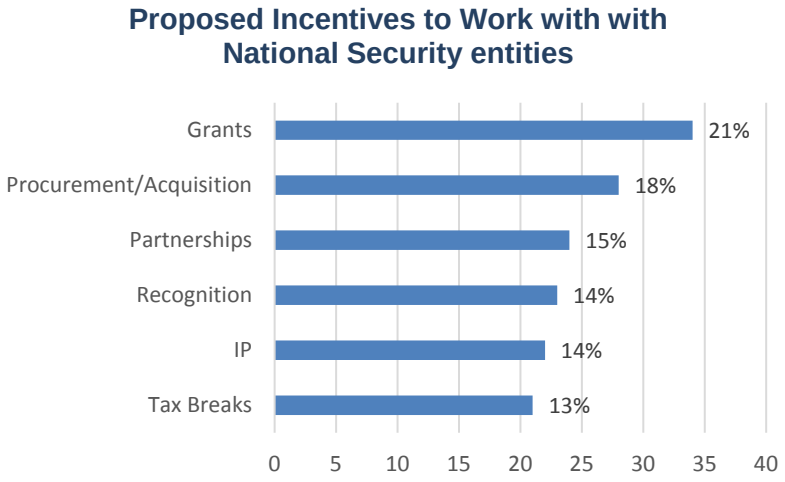

Figure 3: ETNS survey, Incentives to encourage working with national security entities, May 2018

Of lesser importance to respondents were the ideas of individual or company recognition for demonstrating a commitment to national security interests, longer term intellectual property (IP) rights and accesses, and tax breaks.

Technology used for military, intelligence, and other national security roles is not novel, and these sectors have historically been a major developmental driver. However, disputes by private employees and corporations over the use of technology for these applications is a relatively new, and potentially significant, constraint and one most U.S. adversaries do not necessarily have, but with a global footprint, may experience. For example, Amazon's facial recognition program, 'Rekognition,' currently shares information with certain law enforcement agencies. It is an example of technology advancement raising civil, privacy, and ethical concerns about its legal usage and data sharing possibilities.[24,25]

[24] Johnson, Tim, "Big Tech firms march to the beat of Pentagon, CIA despite dissension," *Centre Daily Times*, June 4, 2018 http://www.centredaily.com/news/nation-world/national/article212173259.html#storylink=latest_side
[25] *See, e.g.* Cagle, Matt and Nicole Ozer, "Amazon Teams Up with Government to Deploy Dangerous New Facial Recognition Technology," ACLU.org, May 22, 2018 https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new

Is this the future for public-private partnerships?
From 'lack of recognition' to 'outright non-participation'?

In May 2018, Google decided not to renew a DoD contract after some employees objected to work the firm was doing for the U.S. government. According to Money magazine, 4,000 (of 88,000) Google employees signed a petition to demand, "…a clear policy stating neither Google nor its contractors will ever build warfare technology" and twelve employees apparently resigned in protest.[26] The DoD project that Google was contributing to, referred to as Project Maven, is an artificial intelligence initiative that uses AI to process the voluminous video captured by the DoD in its missions around the world, including footage captured by unmanned aerial vehicles. The goal of the project was to produce "actionable intelligence and insights at speed"—to better identify adversaries such as ISIS and ensure targets are appropriately identified. [27,28]

The Google corporate decision is an example of a private sector participant unwilling to sell its services to or participate in a U.S. national security initiative. It is too early to tell if this represents a trend for other companies, but the decision does raise many new questions about the future working relationship between the defense and intelligence community and private industry.

As individuals and corporations reconsider how they will engage with the U.S. government on national security-related matters and how that relationship aligns with their own global business models and ethics and civil liberty positions, the government may have to reconsider how it engages with private industry and the global marketplace through its research and development, investment, partnerships, and commercial contracts. The working relationship between the U.S. government and the private sector is important. To strengthen this relationship, the U.S. government should highlight the economic

[26] Byers, Dylan, "Google says it will not renew controversial Pentagon contract", Money.cnn.com, June 1, 2018 http://money.cnn.com/2018/06/01/technology/google-maven-contract/index.html
[27] Johnson, Tim, "Big Tech firms march to the beat of Pentagon, CIA despite dissension," *Centre Daily Times*, June 4, 2018 http://www.centredaily.com/news/nation-world/national/article212173259.html#storylink=latest_side
[28] Byers, Dylan, "Google says it will not renew controversial Pentagon contract", Money.cnn.com, June 1, 2018 http://money.cnn.com/2018/06/01/technology/google-maven-contract/index.html

advantages, educational benefits, and the value of private sector cooperation to achieve national objectives.

The National Security imperative for emerging technologies and partnerships

To advance U.S. competitiveness and national security interests, the following steps are needed to help the U.S. develop, implement, and protect emerging technologies:

- Identify the U.S. technology blueprint needed for the future;
- Understand the actions and areas of opportunities for U.S. interests and track those exploited by other countries;
- Explore worldwide science and technology trends, attract and retain inventors and innovators, leverage private capital and expertise to build and innovate, and rapidly field inventions and innovations;
- Develop the workforce for today and the future; and
- Acknowledge software as a national, corporate asset to be protected and harnessed.

The 2017 National Security Strategy (pp 20-21) identified the U.S. intention to lead in Research, Technology, Invention and Innovation. The strategy states, "The U.S. will prioritize emerging technologies critical to economic growth and security, such as data science, encryption, autonomous technologies… AI..." In doing so, the NSS intends to promote and protect the U.S. National Security Innovation Base.[29]

The DNI Worldwide Threat Assessment published in February 2018 concluded that new technologies and novel applications of existing technologies have the potential to disrupt

[29] "The National Security Strategy of the United States of America," The White House, December 2017, pg. 20 https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

labor markets and alter health, energy, and transportation systems.[30] Furthermore, it stated that technology acquisitions and strategic economic competition, "…will continue to challenge U.S. economic security."[31] This will influence further trade imbalances and barriers, while certain countries will continue to acquire (illicitly and legally) U.S. intellectual property and propriety information to further their own economic and national security goals.

While the NSS and Worldwide Threat Assessment recognize the pressures associated with today's geopolitical and economic environments, there is a difference between acknowledging the vulnerabilities and implementing large scale, strategic shifts to offset competitor and threat activities and approaches aimed at the U.S.

Action and results follow a robust strategy and committed culture. The U.S. and its technology partners can and should identify U.S. strategic technological needs and create a national strategy. Using history as a guide, President Dwight Eisenhower signed the Federal-Aid Highway Act of 1956 which created a 41,000-mile "National System of Interstate and Defense Highways" that would, according to Eisenhower, eliminate unsafe roads, inefficient routes, traffic jams and all of the other things that got in the way of "speedy, safe transcontinental travel." The highway would also serve a secondary purpose, "in case of atomic attack on our key cities, the road net [would] permit quick evacuation of target areas." This highway concept was therefore identified as "essential to the national interest."[32] That same strategic perspective and singular focus should be applied to technology achievements that are "essential to current and future national security interests." Once defined, the road map can be developed for specific initiatives.

Through the team's research and discussions, particularly during its research trip to San Francisco, a consistent theme emerged—that the U.S. needed to put an "aspirational stake" in the ground terms of its strategic technological intent, economic competitiveness, and national security goals. Given that observation, the commitment to a modernized, innovative

---

[30] Coats, Daniel R., "Statement for the Record, Worldwide Threat Assessment of the U.S. Intelligence Community," Office of the Director of National Intelligence, February 13, 2018, pg. 12.
[31] Ibid.
[32] The Interstate Highway System, Author History.com Staff, Website Name History.com, Year Published 2010 Title: The Interstate Highway System, URL http://www.history.com/topics/interstate-highway-system, Access Date May 07, 2018, Publisher, A+E Networks.

technology strategy comparable to the national highway system of the 1950's or the U.S. strategic, single-focused scientific and technological mission response to the USSR's Sputnik 1 success is critical to sustaining the U.S. position within the global marketplace and geopolitical spectrum.

Technology Projections and U.S. Posturing

*The study team summarized that the U.S is at an **"inflection point"** in terms of sustaining its global economic and technological position and maintaining its competitive edge.*

Based on the ETNS survey, the items captured in Figure 4 were identified as the most critical emerging technology fields in which the U.S. should be investing.

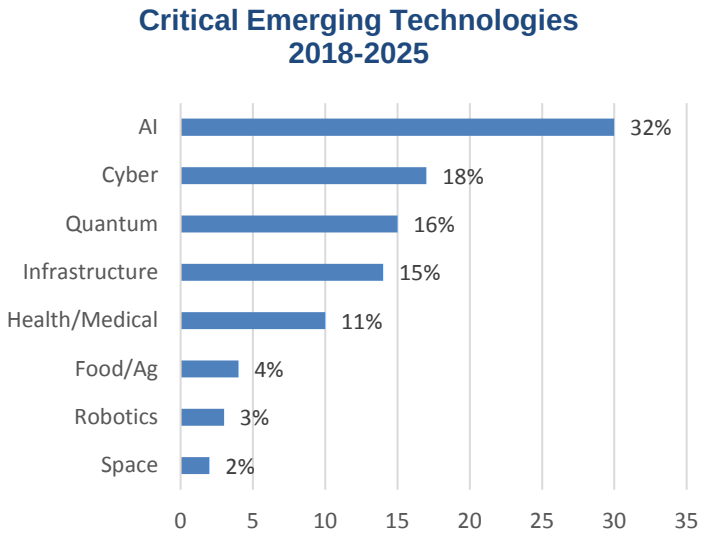

Figure 4: ETNS Survey, May 2018

These offer opportunity and advancement; however, investments must be conducted with targeted goals in mind and within an environment that encourages the transfer of people and knowledge. Creating investment grants and reversing the decline in government R&D investment could encourage greater, and more effective, public-private partnerships.

The ETNS team identified several contributing factors to use in its analysis to develop the "plausible futures" model based on R&D agility and geopolitical focus (Figure 5).

Agility of Federal R&D Involvement

Federal involvement in R&D provides vital funding and organizational arrangements which could encourage innovation, often with positive spillover effects to the wider economy.[33] The historical impact of these arrangements becomes apparent when one considers that "every technology that makes the iPhone 'smart' (Internet, GPS, touch-screen display, and SIRI) was publicly funded…."[34] Despite the historical importance of government R&D investment, funding allocated for basic and applied research has decreased, as mentioned above.

While overall federal funding is important, it is not sufficient to ensure an innovative technology ecosystem.[35] This is especially true in technologies, such as artificial intelligence, which require more collaboration between the government and the private sector. While the global competition can influence the dynamics of collaboration, the US government has created special arrangements, including the Pentagon's Defense Innovation Unit-Experimental (DIUx) and the Central Intelligence Agency's In-Q-Tel, to enhance collaboration between civilian and government technology sectors; however, these "programs are tiny compared to the behemoth of traditional federal acquisitions," that favor large, traditional defense contractors.[36] It is also not clear through the team's study to date

[33] Weiss, Linda. America Inc.?: Innovation and Enterprise in the National Security State. Ithaca, NY: Cornell University Press, 2014.
[34] Mazzucato, Mariana, *The Entrepreneurial State: Debunking Public Vs. Private Sector Myths*, Anthem Press, June 10, 2013.
[35] Evans, Gareth, "Is the US military machine losing its innovation edge to China?", Army-technoloy.com, March 29, 2018 https://www.army-technology.com/features/us-military-machine-losing-innovation-edge-china/
[36] Carter, William, "Statement Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities 'Chinese Advances in Emerging Technologies and their Implications for U.S. National Security', January 9, 2018 https://docs.house.gov/meetings/AS/AS26/20180109/106756/HHRG-115-AS26-Wstate-CarterW-20180109.pdf

whether there is an overall strategic, coordinated approach to these programs and their investments or if they are instead a collection of individual projects that may or may not contribute to national security strategic objectives. The study team believes this is an area of further discovery and a topic for a follow-on effort.

Focus on Strategic Priorities

Innovation is in part driven by how focused—or diffuse—the United States' attention is to geopolitical threats; the clearer the focus on an adversary, the more innovation could occur. In the words of one author, "…this is a game as much about focus as capability."[37] The importance of focus is well-illustrated by many modern technological breakthroughs with origins in geopolitical struggles, ranging from space flight to the computer.[38] The process that brings a threat to the national psyche can be immediate or gradual. In the case of the former, the launch of the then-USSR's Sputnik satellite immediately increased concerns about the Soviet missile program and led to a push for numerous US science and technology investments. More recently, the September 11 attacks led to innovations in unmanned aerial vehicles and surveillance technologies to combat asymmetric threats.[39]

The Spoiler Effect of U.S. Domestic Politics

Domestic policies impact the agility of federal R&D efforts. Since the next generation of technology requires a high level of engagement with civilian partners, maintenance of these relationships is crucial. Controversies such as the Edward Snowden leaks can create negative public relations for companies that collaborate with the government, and subsequently draw them away from federally-sponsored projects. Concurrently, the government reputation is impacted for its use of technology and specific polices. As previously mentioned, Project Maven is an example of these scenarios, as Google employees expressed concern that the project is counter to the company's philosophy of

[37] Evans, Gareth, "Is the US military machine losing its innovation edge to China?", Army-technoloy.com, March 29, 2018 https://www.army-technology.com/features/us-military-machine-losing-innovation-edge-china/
[38] Ratner, Andrew, "War sparks leaps of technology," *Chicago Tribune* http://www.chicagotribune.com/news/nationworld/sns-worldtrade-technology-ss-story.html
[39] Ackerman, Robert K., "War on Terror Drives Dynamic Military Innovations," *SIGNAL*, April 2006 https://www.afcea.org/content/war-terror-drives-dynamic-military-innovations

"don't be evil."[40] Other critics of government-private sector technology projects contend collaborations like Project Maven hamper the innovation process.[41]

Partisan politics also impact the ability of the U.S. to maintain geopolitical focus on its adversaries. During the Cold War, the threat of the then-Soviet Union led to a bipartisan consensus on the need to invest heavily in science and technology for national defense.[42] When the Berlin Wall fell, U.S. federal investment declined as national security concerns decreased. In today's ever changing political and technological environment, the need for agility to adapt national security technologies and strategies has become imperative.

Plausible Futures Model of U.S. Innovation Competitiveness for National Security Technologies

Based on the drivers above, and considering the impact of domestic policies, the ETNS team developed four plausible futures of U.S. innovation competitiveness for national security technologies over the next decade (Figure 5). These futures are not mutually exclusive; it is possible various elements of these could intermix to produce other combinations.

[40] Wakabayashi, Daisuke and Scott Shane, "Google Will Not Revew Pentagon Contract That Upset Employees," *The New York Times*, June 1, 2018 https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html
[41] Malcomson, Scott, "Op-ed: Why Silicon Valley Shouldn't Work With the Pentagon," *The New York Times,* April 19, 2018 https://www.nytimes.com/2018/04/19/opinion/silicon-valley-military-contract.html
[42] Cohen, Linda R. and Roger G. Noll, "Is U.S. Science Policy at Risk?: Trends in Federal Support for R&D," *Brookings*, December 1, 2001 https://www.brookings.edu/articles/is-u-s-science-policy-at-risk-trends-in-federal-support-for-rd/

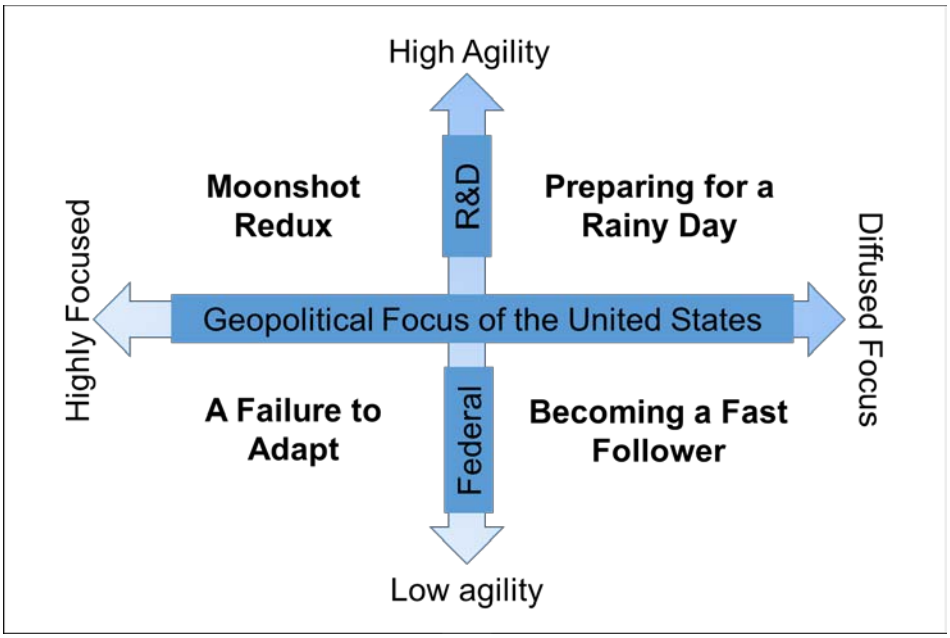

Figure 5: Plausible Futures of U.S. Innovation Competitiveness for National Security Technologies

"Moonshot Redux"

In this scenario, concern over near-peer rivals, specifically China, creates a domestic political consensus to increase investments and reform the U.S. R&D base. Such a consensus would be forged in the aftermath of a focusing event on par with the September 11, 2001 attacks, a cyber "Pearl Harbor", or a low intensity skirmish in the South China Sea. In either hypothetical case, the U.S. would be shown to be behind in a key technological area, a possibility that is not altogether implausible; experts suggest the U.S. could be lagging in critical areas, such as quantum computing.[43] To respond to the geopolitical threat in this scenario, a domestic consensus would better allow the U.S. to set forth a strategic plan for technology development and increase investments in R&D, as well as shift towards "fresh thinking" on acquisition and procurement. In the case of the latter, new forms of collaboration would increase agility. Concurrently, policymakers could pass legislation

[43] Carter, William, "Statement Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities 'Chinese Advances in Emerging Technologies and their Implications for U.S. National Security', January 9, 2018, pg. 2 https://docs.house.gov/meetings/AS/AS26/20180109/106756/HHRG-115-AS26-Wstate-CarterW-20180109.pdf

similar to the 1958 National Defense Education Act, which occurred in response to concerns about Soviet capabilities and allocated increased funding for higher education in STEM. These initiatives would allow the US to retain its position as the lead technology innovator for the foreseeable future, provided this focusing event occurs early enough that the U.S. has not already fallen too far behind.

"Preparing for a Rainy Day"

This future sees the US acknowledging the need to reform the technological ecosystem, despite not having a clear military geopolitical threat to focus on. While this outcome seems unlikely, it has happened before. During the 1970s and 1980s the U.S. began focusing on dual-use technologies to counter the rise of Japan's microelectronics industry. This led to intellectual property reform, new procurement programs, and a "merging of public and private innovation efforts."[44] Similarly, in this scenario, US policymakers realized the threat associated with falling behind in key technologies and enacted wide-ranging reforms similar to those in the aforementioned scenario. The boost from these reforms could allow the U.S. to stay ahead in most, if not all, key technologies past 2030.

"A Failure to Adapt"

Similar to "Moonshot Redux," the U.S. could face a focusing event that shows its technological capabilities to be lagging. However, in this scenario, the U.S. does not make its R&D efforts more agile, or the event occurs too late for the U.S. to catch up. Instead, it continues the same relatively slow-moving approach to development, procurement, and acquisition that was successful during the Cold War. Some argue the U.S. took this approach at the beginning of the Global War on Terror. While there were significant increases in government funding, especially for the biological sciences, questions remained regarding the overall direction of spending. In particular, technological innovation centered on the important – but relatively narrow – goal of improving the warfighters' capabilities to fight asymmetric threats. Specifically, the Defense Science Board "lamented the lack of a

[44] Weiss, Linda. America Inc.?: Innovation and Enterprise in the National Security State. Ithaca, NY: Cornell University Press, 2014 p. 43.

coherent forward-looking vision for a twenty-first century net-centric fighting force."[45] In this scenario, the US would likely slowly cede the lead across many types of technology. Additionally, the domestic political landscape could prompt some private-sector partners to refrain from collaborating with government R&D efforts. As a result, the U.S. would be ceding its technological leadership to China by 2030.

"Becoming a Fast Follower"

In this worst-case scenario, the lack of a clear geopolitical focus combined with an inability to adapt R&D developments causes the U.S. to lose its competitive edge in innovation. The geopolitical threat from China is not realized for a couple of reasons in this scenario. First, partisan polarization draws U.S. attention inward to domestic disorder. The U.S. does not attempt to reform or improve its R&D technology system due to the domestic disorder and lack of strategic focus. Second, China remains relatively stealthy in its attempts to surpass the U.S. as the global innovation leader. It could do this by continuing to keep much of its development capacity off-shore.[46] Significant cuts also occur to basic and applied research as concerns about budget deficits increase. By the end of the decade, the U.S. becomes a fast-follower behind China in most technology areas. Over time, in this scenario, the U.S. will simply be outpaced by China, due to lack of agility in development, stymied innovation, and limited resources.

All of these options have pros and cons associated with them which are complex, and involve some factors that are uncontrollable or unknowable. However, they also represent a decision point, or inflection point, for the U.S. to choose a direction and develop a strategy for the innovation and technology competition the U.S. wants to contend, or be a world leader, in. Having a direction provides the public and private sectors the knowledge of what the investment boundaries are, from the government's perspective, and what is reasonable or attainable in terms of pace, innovation, investment opportunities, and technology challenges.

---

[45] Weiss, Linda. America Inc.?: Innovation and Enterprise in the National Security State. Ithaca, NY: Cornell University Press, 2014, p. 49.
[46] Weiss, Linda. America Inc.?: Innovation and Enterprise in the National Security State. Ithaca, NY: Cornell University Press, 2014, p. 232.

Recommendations

The study team recommends that the United States jointly create a more informed, deliberate, and coordinated approach with industry, investors, and technologists to develop and deploy emerging technologies through effective partnerships. These partnerships should encourage and incentivize U.S. economic, technology, and national security interests to contribute to the competitiveness of the nation for the future.

The U.S. Government should:

- Recognize the urgency associated with the global competition for technology and economic superiority; commit the appropriate resources; contribute to the environment that leverages the best from the U.S. innovation and educational base; and expand and modernize the processes for development and dissemination of technology.
- Select and commit to a strategy for investment and then effectively integrate policy, technology, and resources from public and private sectors to successfully enable and posture the U.S. to remain competitive.
- Offer incentives and measures to drive, encourage, and stabilize technology developments within the U.S.
- Institutionalize the public and private stakeholder relationships to benefit the workforce, provide opportunity, contribute to economic growth, and protect national security interests.
- Explore new approaches for technology design, development, and implementation concepts that are effective and streamlined to manage risk while improving agility

and speed to market. Some examples identified by the team include[47]:

- Think big, start small, act fast
- "Run, trip, run"
- De-risk, Deploy, Scale
- Design, test, build (repeat)

From the study team's survey, the following policy/process changes would be most effective to enable emerging technologies in a national security context.

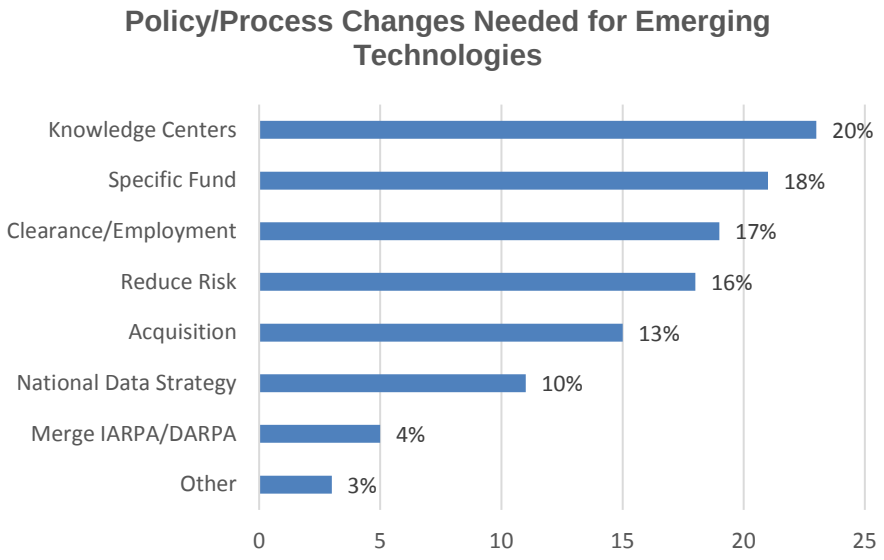

Figure 6: ETNS Survey, May 2018

[47] The study team saw examples of these developmental approaches in action during its research to Silicon Valley and in conversation with other venture capitalists. These models are not something commonly replicated, or currently used within government, but may need to be piloted with modified risk parameters. Encouraging and accepting some risk, and learning from risk instead of considering it failure, is a mind-set and cultural change that is widely accepted by innovators and technologists, but not generally by government decision makers or project leads.

Derived Key Suggestions:

Create Public-Private Knowledge Centers

These facilities would host government and private sector individuals who can interchange jobs and knowledge over a career for continuous development and contribution. There has been an uptick in similar constructs throughout Europe of similar efforts, as stated earlier, with immediate success. This construct would require a revamped and modernized security clearance process that enables the transition between government and industry positions more easily. This joint effort would provide a measurable, effective difference in how government and industry jointly approach emerging technology development and implementation for national security initiatives that benefit the U.S. writ large. Associated with this action is the critical need to revamp and **modernize the security clearance processes** and employment policies to employ individuals within government and industry more interchangeably.

Establish an emerging technology investment fund

This is loosely defined as a large-scale hybrid mechanism to make both early and later stage investments in various equity securities, allowing for U.S. taxpayer dollars to combine with private capital. It would have a two-pronged investment thesis of assisting the government maintain its precarious technological superiority position, and also driving value for investors. Well-resourced adversaries for years have used their sovereign investment funds (through state owned or directed enterprises) to buy or gain influence over critical technology companies and nascent industries both in the U.S., but more alarmingly as of late, overseas, where foreign government incentives are attracting technology cluster formation in ways the U.S. is unable to replicate. Without a comparable mechanism, or different approach to enable influence and deny ownership, adversaries will continue to exploit their government controlled commercial activity tools to buy their way to technological superiority and economic gain.

This private-public technology investment partnership could also (using initial government subsidy and support) enable investment in projects where the opportunity is very nascent, or risky, yet if realized, potentially game-changing to national security. Various constructs can also be developed to ensure that US taxpayer money is protected and accounted for

throughout the process.

Evolve and modernize acquisition programs and processes

Opportunities exist to develop new emerging technology-centric, government-wide acquisition processes based on the successes of Other Transactional Authorities (OTA). In the short-term, maximize the use of OTAs within the government's acquisition community to work between the traditional acquisition processes. OTAs can be used to build prototypes of systems outside of the Federal Acquisition Regulations with greater ease and flexibility. Accelerate the startup process by providing revenue or incentives to investors which adds value to the company and attracts partnering. Improve speed to market for the benefit of all stakeholders.

Directly address civil liberty, privacy, and ethical concerns and impacts

Modify and address civil liberties, privacy, and ethical impacts vs. national security concerns in a more robust, forward-thinking manner related to the development and implementation of emerging technology within the national security sector. Whether these factors could lead to the government conducting more R&D internally if companies and individuals believe it is not acceptable to use their technology advancements for war time or national security applications is something that needs to be monitored and factored into the technology development decision process.

Develop and leverage internal, available US resources and talent

The U.S. should recognize the strength and capability of U.S. labor and talent and not aspire to replicate the models employed by adversaries. Government and industry incentives that encourage U.S. students to study STEM are important. Also important is capitalizing on the U.S. entrepreneurial spirit, the desire of Americans to innovate, to solve problems, and be creative in a manner that promotes economic growth and technology advancement.

Create a clear, succinct US National Strategy for Emerging Technologies

A strategy that includes targeted investment programs and opportunities to encourage interest and public/private participation within this sector is important. Partnering with industry to enact proactive policies that stimulate technology development and innovation within the U.S. is beneficial for all. Develop U.S. government incentives and grants for basic

research investment funding and targeted, specific projects for technologies to achieve. Create pro-growth and productivity enhancing economic policies.

Transform the 2017 NSS into an aggressive action plan

Adversaries are equally interested in winning the race for technological and economic superiority; and the best resourced of them have more tools at their disposal to build or buy the technologies that will matter most in this race. No longer can the U.S. rely solely on the promise of American ingenuity (or loyalty) inside its borders. It needs to adapt and adopt key technologies that it considers vital for the future US technology and economic standing, jointly develop specific, targeted strategies to achieve the priorities identified.

The ETNS team concluded that the U.S. has an opportunity to leverage its own resources and talent, in a manner that promotes economic growth and technology advancement that does not have to replicate models of competitors or allies. A clear, succinct U.S. National Strategy for Emerging Technologies, with targeted investment programs and specific opportunities, could maximize interest and public/private participation within this sector to achieve U.S. national security goals, technology advancements, and economic benefits.

Team Members

Stephen Coulthart, University of Texas, El Paso National Security Studies Institute, Co-Team Lead

Lorri J., National Security Agency, Co-Team Lead

Robb B., ODNI/National Counterintelligence and Security Center

Jordan Hansen, The Boeing Company

Everett Hinkley, USDA Forest Service

Catarina Kim, CK Consulting Inc.

Daniel Paltiel, U.S Bank

Tony Porter, Eastern Foundry

Ian Schade, New York County District Attorney's Office

James Smith, Ankura Consulting

Sarah Soliman, RAND Corporation

Elizabeth R., ODNI Champion