Prepared Statement by

DJ Patil, Ph.D.

Senior Fellow, Belfer Center for Science and International Affairs, Harvard Kennedy School; Former U. S. Chief Data Scientist; Former member of the National Infrastructure Advisory Council

Before the

The House Permanent Select Committee on Intelligence's Subcommittee for Strategic Technology and Advanced Research Hearing on "Emerging Technologies and National Security: Posturing the U.S. Intelligence Community for Success"

Chairman Himes, Ranking Member Stewart, and members of the STAR sub-committee, thank you for the opportunity to testify on this important subject.

The success of the Intelligence Community (IC) is deeply personal to me. On September 11, 2001 at the University of Maryland, I was conducting research into how to use massive datasets to find patterns in the data. After watching the tragedies at the Pentagon, the World Trade Center, and a field in Pennsylvania; I was determined to change my career trajectory in order to serve my country. At the time I had been working on ideas of how we could use the increasing volume of data to understand patterns that might be otherwise hidden.

Our research group had strong name recognition and a track record of success in applied science, but it was a challenge to find ways to work with the intelligence community. Despite the 9/11 Commission's recommendation to use data more effectively[1], it took me until 2004 before I was able to to join the Defense Threat Reduction Agency (DTRA) under the Department of Defense in President G.W. Bush's Administration. I am proud of our work at DTRA and the foundations it laid for our national security enterprise to be ahead of what we now call the big data revolution.

[1] 9/11 Commission Report https://www.9-11commission.gov/report/911Report.pdf pp 416-419 including the recommendation "The President should lead a government-wide effort to bring the major national security institutions into the information revolution"

The risk is losing is real

The world as we know it is changing faster than ever and the primary driver of that change has been innovation in the U. S.. Consider what the world looked like over the past decade from a few popular brands and products:

- 2007: iPhone, Kindle, and Airbnb launch
- 2008: Tesla Roadster launches
- 2009: Turn-by-turn directions on phone; and WhatsApp and Uber launch
- 2010: Videos on mobile phones are adopted; Pinterest, Instagram and ipad launch
- 2011: Snapchat launch
- 2012: Lyft and Tesla Models S launches

They are all U. S. based companies that produced these products and companies. Collectively they have had a staggering impact on our society, transforming the way we consume content, interact, and experience the world. Behind all of these products are advancements in technology from increasing power of computing, storage, and batteries. And given the advancements we expect to see from genomics, AI, data science, to quantum computing, the world as we know will be radically different in the next decade.

These advancements due to our national research and development (R&D) strategy, immigration, investment, etc. But what happens in an increasingly global world with easier access to technologies? We are already seeing the rise of new products that are not based in the U. S. For example, TikTok, a social media platform, has more than 400 million users[2] and is on track to rival major U. S. social media platforms. Huawei, is developing their own operating system to reduce their dependence on Google's Android platform.[3] And there are increasing concerns how these technologies will align with western values. For example, TikTok has censored content the China's government finds objectionable.[4]

As this next phase of globalization develops, it is critical to make sure that the U. S. continues to preserve its competitive and national security advantage with our values intact and perpetuated in the technology we produce and engage with. We must continue to push for higher ideals and standards so that technology works for us and not against us.

---

[2] https://www.bloomberg.com/news/articles/2020-01-19/snap-ceo-spiegel-says-tiktok-could-grow-bigger-than-instagram

[3] https://www.cnet.com/how-to/harmonyos-whats-huaweis-android-replacement-operating-system/

[4] https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing

To look into these issues, I participated in Council on Foreign Relations (CFR) sponsored independent task force and we published our findings in a report; Innovation and National Security: Keeping Our Edge.[5]

This topic is deeply personal to me for a few reasons. First, I'm an immigrant to the U.S. and this country has given me incredible opportunities. Second, I'm trained as a mathematician and science is my first love. Third, having had the opportunity to serve twice in public service, I've witnessed first hand how critical innovation is to national security.

The quote that I think sums it up best is from Ash Carter the 25th Secretary of Defense, "Security is like oxygen, if you have it, you don't pay attention to it".

We've stopped paying attention to it.

As a former public servant, an investor, as technologist and executive in multiple successful technology companies like LinkedIn, eBay, and PayPal; I am deeply concerned about the gap we have created and impact on national security.

For 75 years, the U.S. has led the world in innovation. And we've benefited massively from GPS, touch screens, the internet, data science, to solar panels. The foundation of this has been research sponsored by the U.S. Federal Government. But now we risk falling behind other nations. U.S. federal R&D as a percentage of gross domestic product (GDP) peaked at above 2% in the 1970s and has declined since, from a little over 1% in 2001 to 0.7% in 2018.

Take for example the National Laboratories, administered by the Department of Energy (DOE), are among the crown jewels of research in the United States. These seventeen labs began as a result of the increased funding for scientific research during World War II. The most well-known lab is Los Alamos, where the research into and development of the atomic bomb took place. But there is a long list of notable scientific and technical discoveries across all the labs, including the discovery of twenty two chemical elements, the running of thirty-two of the five hundred fastest supercomputers, the provision of computational infrastructure for the Human Genome Project, and the development of GPS.[6]

Each year the National Labs receive roughly $12 billion in funding and produce nearly 1,500 inventions and 700 patents. The labs also support the training of graduate students, with resources unavailable anywhere else, including supercomputers and equipment required to study high-energy physics, like advanced particle accelerators. Unfortunately, the current

---

[5] https://www.cfr.org/report/keeping-our-edge/?utm_campaign=innovation-tf&utm_medium=social_earned&utm_source=toolkit

[6] U.S. Department of Energy, 75 Breakthroughs by the U.S. Department of Energy's National Laboratories (Livermore, CA: Lawrence Livermore National Laboratory Public Affairs Office, 2017), http://energy.gov/downloads/75-breakthroughs-americasnational-laboratories.

Administration has recommended a 30 percent cut in funding for the National Labs. However, the labs' scientific track record continues to be strong, and cuts to funding would irreversibly harm the foundation these institutions provide to both national security and American technological competitiveness.[7]

What isn't as obvious is the impact on training on the next generation of scientists and technologists. I spent significant time during graduate studies at Los Alamos. And I'm grateful for the experience and mentorship. Contrary to the belief that industry is the primary driver of innovation, many of the seminal in data science were derived from work at the National Labs.

As we look across the international landscape of innovation, the status quo is about to change and the impact will be massive. China is investing heavily, having increased its R&D expenditures by an average of 18% annually since 2000. China already graduates almost three times the number of undergrads with degrees in science, technology, math, and engineering than the United States. And Beijing soon will be one one of the leading powers in emerging technologies. Additionally, as the barriers to technologies are lowered, we'll see non-state actors adopt technologies in new ways with potentially destabilizing impacts.

To be blunt, we face a real risk of falling behind China in science and technology innovation in critical areas, and if we do, the national security and economic consequences could be severe.

We have fallen behind in certain critical technology areas before, most notably in nuclear technology to Nazi Germany during World War II and in space technology to the Soviet Union with the launch of Sputnik in the 1950's. But in both cases we mobilized, leapt ahead in basic research and reestablished our leads much more strongly than before. This is what we need to do now.

We also have a cultural problem that we need to recognize. While there always has been a gap between the policy and technology communities, political disputes over immigration, climate change, and other issues have widened the distance. Silicon Valley and Washington increasingly view each other with distrust. And that slows progress as well as hinders national security.

Finally, our ability to attract, retain, and develop talent is central to the U.S. dominance in science and entrepreneurship. Many of our Nobel Prize winners are immigrants and so are the founders of many notable and admired companies. Yet, the U.S. is seeing a decline in its ability to attract highly educated immigrants, and the number of new international students enrolling at American institutions fell by 6.6% during the 2017– 18 academic year, after a 3.3% decline the year before. And we're not fully utilizing American talent, either. Minorities and women remain underrepresented in STEM fields. Only 2.2% of Latinos, 2.7% of African Americans, and 3.3%

[7] Philip Rossetti, "Publicly Funded National Labs Important to U.S. Innovation," American Action Forum, February 14, 2018, http://americanactionforum.org/research/publicly-funded-national-labs-still-important-u-s-innovation.

of American Indians and Alaska Natives hold a university degree in STEM fields. Women constitute 47% of the overall workforce but only 28% of the science and engineering workforce, and women in tech jobs leave the field at a rate 45% higher than men[8]. Genius is evenly distributed, but, to our detriment, opportunity is not.

Igniting the spark of innovation

It is easy to believe that the big data movement was driven by Silicon Valley[9], but in fact many of those that were at the forefront of "big data" innovation were similar to me. They were scientists, mathematicians, and technologists who wanted to do something for their country and undertook a "tour of service" in national security in the IC, the Department of Defense (DOD), the Department of Energy (DOE), and the National Laboratories. After public service we had leading roles at well known startups and were driving large open source projects. And in 2008, we realized that there was a new role that was needed in industry and in government: the data scientist. Little did I realize that calling ourselves data scientists would have been the beginning of a new field[10] and now even a college major.

With the rise of data science, the Federal Government has recognized the value of data scientists. This includes career paths in data science at organizations like the CIA[11], establishing Chief Data Officer or Chief Data Scientist roles within Federal Agencies as part of the H.R.4174 - Foundations for Evidence-Based Policymaking Act of 2018[12], and President Obama's decision to create the role of the Federal Chief Data Scientist within the Executive Office of the President [13] with the mission to "responsibly unleash the power of data to benefit all Americans".

We often falsely attribute innovation to industry without recognizing the critical role the Federal Government plays. As Secretary of Defense Ash Carter said on the first visit of a Secretary of Defense to Silicon Valley in over 20 years. "The government helped ignite the spark, but this was the place that nurtured the flame that created incredible applications. I mention this because it speaks to a partnership that has long existed between America's technology sector and its government and defense institutions…a relationship that can continue in a way that benefits us both."[14] From self-driving cars to GPS, the close relationship between industry and the national defense has been critical. And unfortunately, something that we have increasingly taken for granted.

---

[8] https://www.cfr.org/report/keeping-our-edge/
[9] I use Silicon Valley as a generic term for all technical hubs across the U. S.
[10] "Data Scientist: The Sexiest Job of the 21st Century", Harvard Business Review October 2012 https://hbr.org/2012/10/data-scientist-the-sexiest-job-of-the-21st-century

[11] https://www.cia.gov/careers/opportunities/science-technology/data-scientist.html
[12] https://www.congress.gov/bill/115th-congress/house-bill/4174/text
[13] https://www.youtube.com/watch?v=dKHz9LbgRmo
[14] Drell Lecture https://www.defense.gov/Newsroom/Speeches/Speech/Article/606666/drell-lecture-rewiring-the-pentagon-charting-a-new-path-on-innovation-and-cyber/

As a scientist, a technologist, an entrepreneur, an investor, and a public servant; I have worked in various capacities with the national security communities to accelerate the success of their missions and “close the gap” between the agencies and industry.

Closing the gap

As U. S. Chief Data Scientist working with Secretary of Defense Ash Carter, we found that top technical talent had a strong desire to work on national security problems, but didn’t have an easy way to contribute to the mission. Additionally, startups were unwilling to engage with the Pentagon due to the complexity of regulations around procurement and contracting. As a result, the war fighter was not getting access to the top technology.

Under Secretary Carter’s direction we created a number of new programs to bring Silicon Valley and the Pentagon closer together including the Defense Digital Service (DDS)[15] [16] and the Defense Innovation Unit (DIU).[17] [18]

The mission of DIU is to accelerate the adoption of commercial technology throughout the military and growing the national security innovation base. DIU partners with organizations across the DOD, from the services and components to combatant commands and defense agencies, to rapidly prototype and field advanced commercial solutions that address national security challenges. Rather than forcing startups to come to the Pentagon, we established offices in Silicon Valley, Boston, and Austin.[19]

The DDS is a “SWAT team of nerds” working to improve technology across the Department of Defense. They hire world-class designers, engineers, product managers, and bureaucracy hackers from diverse backgrounds to work on high-impact projects at the Pentagon and across the globe.[20] One of the major successes of DDS has been the Hack the Pentagon initiative, where vetted technologists are invited to participate in bug-bounty (a program where white-hat hackers are compensated for finding flaws in technical systems) on government systems.[21]

These programs have made significant headway in “closing the gap” between technologists and the Department of Defense because of strong public support from Secretary Carter and his

---

[15] https://dds.mil/

[16] https://www.defense.gov/Explore/News/Article/Article/1858615/defense-digital-service-delivers-mission-aligned-tech-for-dod/

[17] https://www.diu.mil/

[18] https://www.wired.com/2015/11/secretary-of-defense-ashton-carter/

[19] https://www.diu.mil/about

[20] https://dds.mil/#our-team

[21] https://www.defense.gov/Explore/News/Article/Article/684616/dod-invites-vetted-specialists-to-hack-the-pentagon/

successors, as well from CEOs and investors from Silicon Valley. This has been critical to creating an environment that can foster collaboration and experimentation in order to iterate on a model that works for both sides.

Additionally, it has enabled a model for “tours of duty” in the national security apparatus, where technologists can serve for a period of time in the Pentagon and for public servants and members of the military to serve in Silicon Valley.

We need to encourage more models like DIU and DDS specifically for the IC. Strategic investors like In-Q-Tel[22] are filling some of the void, but much more is needed to increase the collaboration between the IC and Silicon Valley.

We must recognize what is referred to as the “hoodies vs suits” problem. The hoodies, those from Silicon Valley, are often uninformed of the value the IC contributes to national security. The suits, those from the government, don’t have the ability to spend time to understand the rapidly changing culture and models of innovation required as technology changes at breakneck speed. It is essential that we find environments to make this “suits and hoodies”. Our experience was that there are too few programs for either side to regularly engage or develop meaningful partnerships.

One of the keys to the innovative approach of Silicon Valley is the amount of collaboration around technology. Engineers at Google may partner with those at Facebook around an open source project that will benefit both companies. An example of this is a technology called Hadoop which has revolutionized the way data is processed and it is used by many of the top companies around the world. Much of this early development was done through conferences and informal meetings. And in those conferences it is rare to find a technologist from the IC. I have personally encouraged many data scientists in IC to go to specific conferences to help on problems they are working on. Unfortunately, it is still rare to find IC technologists who travel to the major technical conferences or develop the relationships with technologists in the design of new ideas. The result is that this leaves the IC to build “on an island” without the collective wisdom of the industry.

It is also important to note that there have been attempts by the IC to provide their technology to industry.[23] Many of these projects are excellent, but the challenge has been that they are released with little engagement with the community and as such they do not receive the engagement they should.

The IC should be applauded for their creation of a data scientist career path.[24] I have met with many career data scientists in the IC and they are top quality. And time and time again, I’ve

[22] https://www.iqt.org/
[23] https://code.nsa.gov/
[24] https://www.cia.gov/careers/opportunities/science-technology/data-scientist.html

heard that they want to ensure their job titles have parity with roles in industry. This must continue to be a priority to attract and retain top talent.

Increasing interagency collaboration

In my role as U. S. Chief Data Scientist, one of my objectives was to increase the collaboration across the Federal Agencies around the use of data and associated technologies. To facilitate collaboration, one of the programs we established was the Data Cabinet. This is a group of civil servant data science leaders that would meet periodically to share best practices, identify challenges, and work collaboratively on projects that would mutually benefit respective missions.

We also convened a classified Data Cabinet to support the IC. The meeting rotated between IC hosts and was extremely successful at fostering collaboration among the Agencies. After each meeting there were many actionable results where additional teams were identified and put in contact to share technical solutions and processes.

One of my regrets was not establishing more “moonshots” for IC around technology. For example in establishing the Cancer Moonshot Project or the Precision Medicine Initiative, we were able to create a broad interagency process that included groups as diverse as the National Institutes of Health (NIH) to the National Aeronautics and Space Administration (NASA). The calling for a moonshot helps align Federal resources and personnel in a remarkable way. This takes place through interagency process, budgetary alignment, and enabling public servants to get out of their buildings to engage with each other.

I believe that if we create more moonshots that enable the IC to engage to find new innovative approaches, we would see increased levels of technology in support of their respective missions.

Ensuring the ethical use of data

In 2015, when developing the role of the U. S. Chief Data Scientist, the mission statement was carefully constructed to include the responsible use of data. This was in anticipation of the incredible impact data and technology would continue to make. And in just a few short years we have seen both the powerful benefits in the use of data (e.g., cancer research) as well as data being used to marginalize and harm groups and people.

These ethical challenges of data are not new. During World War II, the Nazis used data and early computers to identify and persecute Jews and people of Jewish ancestry. One of the notable stories is of Rene Carmille who ran the equivalent of the census in France. He realized the Nazi’s wanted to use the census data to round up French Jews. He hacked the machine to prevent the data from being used. And when the Nazis discovered what this ethical hacker was

doing, they arrested and tortured him, and then sent him to die at the Dachau concentration camp.[25]

There is an increasing amount of research taking place to understand the implications of machine learning and AI algorithms. However, these efforts are in their infancy. In our research and in our experience we found that most organizations are ill prepared to address the coming ethical challenges. To address these issues, I, along with MIke Loukides and Hilary Mason, published the first practitioner's manual on implementing ethics into data science.[26]

I believe the IC agencies and other Federal Agencies should follow the recommendations we outline in our book. In particular, following our “5 C’s framework,” which includes building processes to understand and evaluate *i.* consent for the use of data, *ii.* clarity of how the data will be used, *iii.* control and transparency of the data, *iv.* consistency in usage of the data for algorithms and different use cases, and *v.* consequences and harm of data and supporting algorithms.

To help alleviate the potential ethical issues the IC should develop checklists as they use increasingly sophisticated data science and AI. These checklists are similar to the ones that a surgeon would use to decrease the potential for harm.

Additionally, I would suggest that the IC and other Federal Agencies implement “red teaming” on their data science efforts to assess potential downsides of efforts. This includes the development of techniques to both ensure legal compliance and limit negative consequences. This will require the addition of new roles including more technical lawyers and ethicists.

The ethical use of data is an active area of research and the IC and Federal Agencies will need to share best practices between the agencies. As well as engage with industry and academia.

There are significant challenges ahead to retain our cutting edge of innovation and ensure that technology doesn’t cause harm. We are nasient in our understanding of newer AI techniques like deep learning relative to their adoption. And there are serious questions about how we collect and use data. And as technology is implemented into products, both consumer and for the IC, we will need continued investment to ensure that technology works for us rather than against us.

Recommendations

- The White House, Congress, and academia should develop a twenty first-century National Defense Education Act (NDEA), with the goal of expanding the pipeline of talent

[25] http://theinstitute.ieee.org/technology-topics/cybersecurity/a-history-of-hacking
[26] https://www.amazon.com/Ethics-Data-Science-Mike-Loukides-ebook/dp/B07GTC8ZN7/

in science, technology, engineering, and mathematics. A twenty-first-century NDEA would support up to twenty-five thousand competitive STEM undergraduate scholarships and five thousand graduate fellowships.

- Federal and state governments should make an additional strategic investment in universities. The investment, of up to $20 billion a year for five years, should support cross-disciplinary work in areas of pressing economic and national security interest. The IC should engage in this.

- We should fund moonshot approaches to society-wide national security problems. This would support innovation in foundational and general-purpose technologies, including AI and data science, advanced battery storage, advanced semiconductors, genomics and synthetic biology, 5G, quantum information systems, and robotics.

- The United States needs to make it easier for foreign graduates of U.S. universities in scientific and technical fields to remain and work in the country. Congress should “staple a green card to an advanced diploma,” granting lawful permanent residence to those who earn a STEM master’s degree or doctorate. Congress should also pass the Development, Relief, and Education for Alien Minors (DREAM) Act.

- Congress should pass legislation that permits immigrants to live and work in the United States if they can raise funds to start new companies or even take part in seeding those companies, as Canada has done in recent years.

- Universities, federal and state government, and business should address the under-representation of minorities and women in STEM fields through mentoring, training, research experience, and academic and career advising. They should also provide financial support for room and board, tuition and fees, and books, as well as assessments of job placement opportunities in STEM fields, highlighting employers with clear track records of fairness in hiring, promotion, and pay.

- Federal agencies, the private sector, and universities should be encouraged to work together to support debt forgiveness for students going into specialized technology sectors and public service, in particular those that benefit the IC and national security.

- The federal government should make targeted—rather than sweeping —efforts to prevent the theft of scientific knowledge from American universities. The current approach is inserting fear and paranoia and limits collaboration and progress that we need.

- Congress should establish a new service academy, the U.S. Digital Service Academy, and a Reserve Officer Training Corps for advanced technologies (ROTC-T) to foster the next generation of tech talent. Additionally Congress should provide greater amounts of

loan forgiveness to encourage technologists and other experts to have careers in national security.

- Lifelong career paths should be complemented with more short-term, flexible options. The White House and Congress should bring people from the technology industry into all three branches of the government for temporary rotations. They should also develop new fellowships to encourage the circulation of technologists, military officers, and federal officials between the technology sector and the Defense Department.

- The White House and Congress should bolster and scale technology alliances and ecosystems. Technologists from the IC should be encouraged to participate in conferences and other technical forums to ensure they are staying up-to-date on the latest technical advancements.

- The Director of National Intelligence, as well as each of the IC agencies, should implement Digital Service groups (similar to the Defense Digital Service) that are time limited roles to foster innovative approaches. Members of these teams should include cross functional representation from industry, academia, as well as from across the IC. Members of this team should also be associated with the U. S. Digital Service (USDS) for increased collaboration and sharing of best practices across the Federal Government.

- Congress should encourage the formation of technical interagency groups like the Data Cabinet to convene regularly. These groups should involve participation of at least one of the following: U. S. Chief Technology Officer (CTO), U. S. Chief Data Scientist (CDS), and/or the Federal Chief Information Officer (CIO).

- Congress should encourage the development of technology careers in government that align with the private sector. For example the comparable data science career paths between industry and the CIA.

- To ensure technical oversight and independent assessments, Congress should revive the Office of Technology Assessment (OTA) and staff it strong independent technical leadership. As part of this revival, OTA should be able to provide Congress with input on the ethical implications of technology.

- The IC should develop an ethical review process for algorithms and use of data. They should follow the 5C's model and implement "red teaming for algorithms".[27]

[27] https://www.amazon.com/Ethics-Data-Science-Mike-Loukides-ebook/dp/B07GTC8ZN7/