Weekly Media Report –Sept. 8-14, 2020

Further reproduction or distribution is subject to original copyright restrictions.

9/11:

1. Nearly Two Decades After 9/11, There Are Still Plenty of Lessons of Resilience We Can Learn

(Monterey County Weekly 11 Sept 20) … Marielle Argueza

Lessons in shared resilience from Sept. 11, 2001 can help us in a time of collective trauma today.

The Naval Postgraduate School today, in a 9/11 address, states this hard work of remaining resilient in the face of adversity is something that can unify us—no matter how hard, messy, reactionary, and ugly it can get along the way. The statement reads: "We may never forget the tragedy of 9/11, but remembering it helps to ensure that we strive to do everything possible to build a better world for future generations."

INCLUSION & DIVERSITY:

2. Dialogue Continues as Naval Postgraduate School Advances Inclusion, Diversity Discussions Virtually

(Navy.mil 10 Sept 20) … Mass Communication Specialist 2nd Class Nathan K Serpico

The Naval Postgraduate School's (NPS) senior leadership hosted a virtual discussion with students and faculty on the topic of inclusion and diversity within the institution Aug. 28. The forum provided updates and transparency on how the command addresses and handles these scenarios.

EDUCATION:

3. Esper Announces New Initiatives to Boost U.S. Position in AI Race

(FedScoop 9 Sept 20) … Jackson Barnett

Secretary of Defense Mark Esper issued a warning to adversaries Wednesday: the U.S. military will adopt artificial intelligence first, and do so ethically… The JAIC, along with the Defense Acquisition University and **Naval Postgraduate School**, will also offer a six-week intensive course on applying AI and data science to a range of military operations and logistical challenges. The course is in the pilot stage now but falls in line with announcements from the military branches to increase AI-specific educational opportunities for service members.

4. Making a U.S. Digital Service Academy Work

(War on the Rocks 10 Sept 20) … Harrison Schramm and **Todd Lyons, Naval Postgraduate School Alumni Association and Foundation**

West Point, America's oldest service academy, was founded in 1802. Over the next two centuries, the United States established academies for the Navy, Coast Guard, Merchant Marines, and Air Force. Each offers a rigorous undergraduate education, commissions officers, and requires graduates to serve a minimum tour of duty.

Recently, the National Security Commission on Artificial Intelligence — chaired by former Google chief Eric Schmidt and former Deputy Secretary of Defense Robert O. Work — published 33 specific recommendations to build the country's capability and maintain its advantage in AI. One of those recommendations was to establish a

U.S. Digital Service Academy modeled on the military service academies. The Digital Service Academy would produce trained government civilians to work across the federal government on high-technology issues.

RESEARCH:

5. Navy Researchers Tackling the "Gray Zone" of Sexual Harassment

(WTKR 10 Sept 20)

NORFOLK, Va. - Combating sexual harassment among the ranks has been a focus of military leadership for years, and now they are taking a closer look at what's called "Gray Zone" behavior.

The Navy describes Gray Zone behavior as anything "which falls short of the technical definition of harassment, but most certainly isn't entirely above board."

Researchers at the Naval Postgraduate School have developed a Situational Judgement Test focused on Gray Zone scenarios.

FACULTY:

6. Twilight of the Human Hacker

(PublicIntegrity.org 13 Sept 20) … Zachary Fryer-Biggs

The Joint Operations Center inside Fort Meade in Maryland is a cathedral to cyber warfare. Part of a 380,000-square-foot, $520 million complex opened in 2018, the office is the nerve center for both the U.S. Cyber Command and the National Security Agency as they do cyber battle. Clusters of civilians and military troops work behind dozens of computer monitors beneath a bank of small chiclet windows dousing the room in light… Walker, who declined to be interviewed for this story through his current employer, Microsoft, admired the progress computer systems like IBM's Watson and Deep Mind's AlphaGo had made in playing games like Chess and Go, according to former colleague **Chris Eagle, a professor at the Naval Postgraduate School in Monterey, Calif.**

ALUMNI:

7. Arab American Women in Government – A Conversation

(The Media Line 8 Sept 20)

Join Jennifer Atala of Inara Strategies for an off-the-record conversation with four incredible Arab-American women serving in government.

Nabeela Barbari, a Naval Postgraduate School Center for Homeland Security & Defense alumna, is the Deputy Associate Director of Strategy and Resources within the Cybersecurity Division at the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

8. Leadership Through Homegrown Values

(Army.mil 9 Sept 20) … Ellen Summey

Daniel C. Jeska, a Naval Postgraduate School alumnus, is the subject in the latest edition of the US Army's "Faces of the Force" online series highlighting members of the Army Acquisition Workforce through the power of individual stories.

UPCOMING NEWS & EVENTS:

September 14 – 18: JIFX 20-4
September 15: Quarterly Awards
September 21 – 24: Warfare Innovation Continuum (WIC) Workshop
September 25: Summer Quarter Graduation

9/11:

Nearly Two Decades After 9/11, There Are Still Plenty of Lessons of Resilience We Can Learn

(Monterey County Weekly 11 Sept 20) … Marielle Argueza

Lessons in shared resilience from Sept. 11, 2001 can help us in a time of collective trauma today.

Good afternoon.

Nineteen years ago today, I was a third grader living in the mostly military community of Abrams Park in Marina. I put on my jacket, stuffed my homework in my backpack and yelled for my sisters that it was time to go. We walked alongside other neighborhood kids, like every weekday, to the bus stop to get to George C. Marshall Elementary School.

It was promising to be a beautiful sunny day, despite the morning fog crawling through the surrounding oak woodlands. I had not yet heard that terrorists had commandeered two planes and destroyed the World Trade Center, that another crashed into the Pentagon and another narrowly missed Washington, D.C.

One of the neighborhood kids ran outside, breakfast in hand, approached my sisters and I and began screaming, "We were attacked! They bombed us!" I don't remember much of the recap as filtered through that fifth-grader's world view. But I do remember the conversations on the bus and in the classrooms, the moment of silence after the Pledge of Allegiance and the whisperings of schoolmates, just kids.

"We're going to kill those motherf***ers," said one particularly overzealous classmate. "I hope my dad doesn't get deployed again—we just got here," said my childhood best friend, Melissa. My third-grade teacher, Mrs. Caves, asked us individually how we were feeling.

It was a traumatic experience for all people of the United States that day, and for the children of my generation, who are now adults, it was the first memorable wide-scale shared experience. Past generations had been through the explosions of NASA's Challenger mission or wars or assassinations that accelerated the forced learning of grown-up ideas. The world watches in times of tragedy indeed, but they also learn. They also act.

I learned more in the following days, weeks, months and years about national interest because of 9/11. I gained a new vocabulary: "terrorist," "Islam," "war on terror." I learned about the constant fear of families who had to prepare themselves to be relocated or prepare themselves to be single-parent households because of potential military deployment. My uncle was deployed to Afghanistan twice during the Bush administration. My oldest sister was deployed once during the Obama administration.

I saw the faces of the leaders who led the attacks circulated in the media well into my high school years. I learned in college about the difficult conversations my Muslim friends had to have with their parents about wanting to divorce or distance themselves from their religious identity. I've seen malicious attacks on hijab-wearing students and racist Halloween costumes.

A lot of ugly things about the world that came to the surface of my adolescence were because of 9/11.

Now, almost two decades later, we are in another shared traumatic experience that has the gravity of changing the way we live now and into the future.

I learned 19 years ago about our resilience as humans to help each other, both in the immediate and long-term. In the immediate aftermath of the attacks, thousands of first responders—firefighters, volunteer search and rescue teams, police officers, EMTs—rushed to find survivors. And yes, the feds helped out too; the House and Senate supported bills to provide emergency response aid for affected areas.

And in the long term, even as many criticized the wars and policies that followed, many of my friends and community members went on to grad school to make sure an attack on American soil at this explosive level would never happen again. Many of my own friends, Muslim or not, saw the trauma of stigmatizing and scapegoating one group. Some started conversation groups in their communities dispelling myths about Islam. Others were invited to Ramadan. They did the slow and arduous work of changing people's hearts and minds and healing their corners of the world.

The Naval Postgraduate School today, in a 9/11 address, states this hard work of remaining resilient in the face of adversity is something that can unify us—no matter how hard, messy, reactionary, and ugly it can get along the way. The statement reads: "We may never forget the tragedy of 9/11, but remembering it helps to ensure that we strive to do everything possible to build a better world for future generations."

http://www.montereycountyweekly.com/opinion/mcnow_intro/nearly-two-decades-after-9-11-there-are-still-plenty-of-lessons-of-resilience-we/article_f20d9208-f48e-11ea-b6d0-7789bfd56a3f.html

Return to Index

INCLUSION & DIVERSITY:

Dialogue Continues as Naval Postgraduate School Advances Inclusion, Diversity Discussions Virtually

(Navy.mil 10 Sept 20) … Mass Communication Specialist 2nd Class Nathan K Serpico

The Naval Postgraduate School's (NPS) senior leadership hosted a virtual discussion with students and faculty on the topic of inclusion and diversity within the institution Aug. 28. The forum provided updates and transparency on how the command addresses and handles these scenarios.

"Today is about conversation and about listening," said U.S. Navy Capt. Ed "Tick" McCabe, NPS Aviation Chair. "It's about having those uncomfortable conversations that are essential to forging a more inclusive force. Our mission is to create a culture where every person feels free to bring their unique perspective to bare on our most critical challenges and where that welcoming environment inspires innovation and the achievement of each individual's full potential."

The discussion started with NPS President retired Vice Adm. Ann Rondeau giving an overview of the first inclusion and diversity discussion held weeks prior and setting the stage for the current, noting her own involvement in the Navy-wide inclusion initiative, Task Force One Navy (TFON).

"I have the privilege of being put on to Rear Adm. Holsey's group, Task Force One Navy, which is a Chief of Naval Personnel-led program to understand our inclusion and diversity issues," commented Rondeau.

Group leaders took turns briefing the command about various subjects, like the annual command climate survey, NPS' Inclusion and Diversity Council, human resources and community outreach to local schools. Several leaders from the Monterey chapter of the National Naval Officers Association (NNOA) also spoke about their organization and its dedication to the recruitment, retention and professional development of a diverse officer corps for the sea services.

"Due to NPS' unique student body and in the spirit of inclusion, the NNOA Monterey chapter is looking to include all military branches, as well as junior enlisted personnel stationed at NPS," said NNOA Monterey chapter President U.S. Navy Lt. Brandon Carter. "Group cohesion is going to be a key factor."

The Monterey NNOA is also partnering with the Naval Junior Office Council, a junior officer run forum working with TFON as a one-stop shop that any command can reach out to and receive assistance for diversity, equity, and inclusion points of contact for research and marketing. Also, NPS' Center for Executive Education is developing an inclusive leadership seminar series that looks to create empathetic leaders by providing them with the necessary tools to sharpen their ability to effectively communicate, understand, and lead the diverse members of their future commands.

"The leadership piece has really been the centerpiece for our inclusion efforts," noted McCabe. "We understand that education is the key towards changing culture and changing people."

The meeting also provided a platform for Rondeau to introduce NPS' newest military faculty member U.S. Army Col. Joyce Stewart, who briefly spoke about what she has learned about inclusion and diversity during her 30-year military career.

"Sometimes it's not just the education, but the awareness and just understanding of what you need to do to position yourself to be ready for any opportunities that might be out there," said Stewart.

Following all prepared updates and remarks, Rondeau opened the floor for questions from any and all faculty and students in attendance. She addressed questions about the newly-formed TFON, current events in the realm of inclusion and diversity, and what an inclusive and diverse workplace would look like.

"One thing that NPS can do is be an exemplar of how we teach leadership and how we understand different points of view," stated Rondeau. "Diversity of thought is what we seek. If you look across our schools, our faculty and our students, there is a great deal of diverse thinking here. We also have a long list of theses and studies done by our students and faculty on this issue."

https://www.navy.mil/Press-Office/News-Stories/display-news/Article/2343641/dialogue-continues-as-naval-postgraduate-school-advances-inclusion-diversity-di/

Return to Index

EDUCATION:

Esper Announces New Initiatives to Boost U.S. Position in AI Race

(FedScoop 9 Sept 20) … Jackson Barnett

Secretary of Defense Mark Esper issued a warning to adversaries Wednesday: the U.S. military will adopt artificial intelligence first, and do so ethically.

Department of Defense officials have spoken ad nauseam about their desires to harness the power of AI in an ethical manner. Esper himself previously said it could "change the character of warfare." But Wednesday, during the Joint AI Center's AI Symposium, Esper spoke on the matter with more conviction, declaring that the U.S.'s goal to field AI for military use before competitors will indeed become a reality.

The stakes are high, Esper said. If America isn't the first to adopt AI for military use, it risks letting other world powers with flawed morals use the technology in unethical ways. "We cannot afford to cede the high ground to revisionist powers intent on bending, breaking or reshaping international rules or norms in their favor," he said of the need to field AI first.

During his remarks, Esper announced new initiatives the department has undertaken to boost its development of AI, including the planning of full-fledged live tests of AI-controlled warfighting aircraft, building off recent virtual tests. These tests implementing AI into dogfights would put algorithms in the cockpit of a tactical plane — a major step toward a future where AI is more deeply intertwined into the so-called "kill chain."

Esper added that the DOD is intent on thinking about the ethics and implications of these moves. "AI's role in our lethality is to support human decision-makers, not replace them," he said.

Other initiatives Esper spoke of focused on ensuring the ethical development and use of AI both in the U.S. and abroad. He said the U.S. will lead the way with its ethical principles for AI and take allies along with it.

Next week, the JAIC will launch a 10-country initiative with allies for military-to-military engagements that focus on incorporating ethical principles into the AI development pipeline, Esper said. He called it the "AI Partnership for Defense."

"The principles make clear to the American people, and the world, that the United States will once again lead the way with the responsible development and application of emerging technologies," Esper said, adding that the department intends to grow the program and invite more countries over time.

The DOD is also looking internally to grow its ethical bona fides. Esper reiterated the importance of JAIC initiatives, like the Responsible AI Champions program and other DOD-wide ethics initiatives that the center is working to scale across the military services and components.

The JAIC, along with the Defense Acquisition University and **Naval Postgraduate School,** will also offer a six-week intensive course on applying AI and data science to a range of military operations and logistical challenges. The course is in the pilot stage now but falls in line with announcements from the military branches to increase AI-specific educational opportunities for service members.

"We see AI as a tool to free up resources, time and manpower so our people can focus on higher priority tasks and arrive at the decision point … faster and more precise than the competition," Esper said.

https://www.fedscoop.com/esper-ai-announcements-ai-race/

Return to Index

Making a U.S. Digital Service Academy Work

(War on the Rocks 10 Sept 20) … Harrison Schramm and **Todd Lyons, Naval Postgraduate School Alumni Association and Foundation**

West Point, America's oldest service academy, was founded in 1802. Over the next two centuries, the United States established academies for the Navy, Coast Guard, Merchant Marines, and Air Force. Each offers a rigorous undergraduate education, commissions officers, and requires graduates to serve a minimum tour of duty.

Recently, the National Security Commission on Artificial Intelligence — chaired by former Google chief Eric Schmidt and former Deputy Secretary of Defense Robert O. Work — published 33 specific recommendations to build the country's capability and maintain its advantage in AI. One of those recommendations was to establish a U.S. Digital Service Academy modeled on the military service academies. The Digital Service Academy would produce trained government civilians to work across the federal government on high-technology issues.

Creating a U.S. States Digital Service Academy is an excellent idea. Although digital service is fundamentally different than military service, it too deserves a specialized institution for education and training. For it to be successful, it should be relevant to the needs of the government sponsor, practitioner-focused, and engaged with its graduates throughout their careers. Just as importantly, it will need to avoid the tendency towards academic insularity and the temptation to measure success against its own metrics of performance.

This Is a Good Idea

Fundamentally, gathering the talent in the United States that has both the ability and interest in engaging in advanced computing — to include AI — is a fantastic idea. A Digital Service Academy would focus scarce human resources on establishing the levels of competency that will form the basis for both the education and evaluation of the broader workforce. By providing a common baseline, a digital service will drive the adoption of AI across the Department of Defense and the broader federal government more effectively than current efforts, which are uneven at best. Like the service academies, graduates of the Digital Service Academy would not constitute the majority of the government efforts in AI. Rather, it would serve as a common experiential basis for rapidly disseminating ideas and techniques.

Digital "service" is fundamentally different from most military service opportunities. Military service is insular in the sense that if one is to be a professional at flying military aircraft aboard an aircraft carrier or firing artillery in support of infantry, there are few relevant opportunities to do this outside the government. In contrast, a digital service is and should be porous in the sense that professionals can flow freely between government and industry. This is explicitly stated in the U.S. digital service mission. We suggest that this should be the defining trait of a successful digital service.

This paradigm shift will require governmental leaders to recognize that the value of the digital service increases at each iteration as personnel move in and out of government. The notion that a career in government service that lasts less than 20 years represents some kind of failure is itself a failing idea. Allowing a freer flow between government and industry is a large step and requires cultural change and legislative action in equal measure. The cultural piece is actually more important and will take longer to

implement. It will require the people who make hiring decisions — and are generally long-term government employees — to consider those with less traditional career trajectories. Doing so demands balancing familiarity with the workings of government with the breadth of experience that comes from exposure to industry. Legislation can incentivize cultural change, but it cannot make it happen by fiat.

Congress should pass legislation to establish different pay scales that encourages truly exceptional talent to enter government service, reduce barriers to working with industry for education and research, and provide for a "reserve commission" that supports keeping an active clearance even as the person transitions from government service into industry. Many in Silicon Valley expect to move between an academic stint at a university and the development of their next startup. Similarly, the government should make it easy for someone that just sold their startup to invest their time in sharpening the skills of the federal workforce. This free flow of talent, knowledge, and dissatisfaction with the status quo would dramatically transform the expectations of both faculty and students.

Additionally, the digital service and the academy that supports it would be a first step towards the "whole of government" approaches that are used by the America's competitors — specifically China. Free societies, such as the United States, are typically not responsive to the broad whole of government solutions in the absence of an existential or imminent threat. The digital service is an idea that can achieve the desired outcome and still be in line with the character and values of the United States and the community of democratic nations more broadly.

Balancing Practitioners and Theorists

The fundamental question addressing the development of the Digital Service Academy is not the students. Qualified, energetic students will come, provided the incentive structure for service and the quality of education are evident. However, the "If we build it, they will come" philosophy is not sufficient on its own. The federal government needs to recognize that it is but one player in a truly global competition for AI talent. Financial incentives, such as free or dramatically reduced-cost education, on their own are also probably not sufficient for this select cohort. A focus on service to the nation — and the advantages that such service can provide an early-career professional — is the key.

The fundamental question that will determine the success of the Digital Service Academy is how it will recruit and retain faculty. The Pentagon and the broader federal government are focused on using AI to solve relevant problems for practical purposes and is therefore a practitioner-*focused* vice *theoretical* activity. Practitioners are needed to balance the promises and risks inherent in AI. This focus on AI-practitioners is equally true for government organizations from the Social Security Administration and the Veteran's Administration to the Department of Commerce and the Department of Homeland Security. The key measure of effectiveness of the Digital Service Academy will not be measured in the number of peer-reviewed articles in discipline-specific journals, but in the number of areas where AI transforms currently intractable problems into transparent and repeatable processes that empower leaders and service members to make better decisions. Building AI models in code is messy and involves a high failure rate. Fundamentally, the application of any bespoke technology like AI does not constitute a goal in itself, but it is a useful tool for accomplishing a necessary task. AI is not useful without competent professionals to supervise its use. This realization has direct implications for the way in which faculty are recruited and retained.

It is certainly desirable, and likely necessary, that much of the faculty at the Digital Service Academy have a defined tenure limit, in stark contrast to comparable educational institutions. This would be similar to the model at the U.S. Naval Academy, where the permanent civilian faculty are balanced by rotational, military faculty. In the case of the Digital Service Academy, most of the faculty would likely be civilians. A model for this might be the program managers at the Defense Advanced Research Projects Agency or similar activities in both government and industry. These agencies recognize that when their program managers step away from "the top of their fields … pushing the limits of their disciplines" to join the agency, their skills begin to atrophy. Likewise, a significant portion of the faculty at the Digital Service Academy should continually be refreshed by a deliberate rotation plan that brings in faculty with the latest techniques and sends out faculty immersed in the Defense Department's most challenging problem sets.

This would also address the challenge of some academic institutions that prioritize publishing theoretical journal articles over the education mission or the focus on exploiting AI to solve the emerging challenges facing the United States.

One approach is to recruit an initial cadre of instructors from government, academia, and industry with a defined term of four years, synchronizing them with a graduation cohort. Having a group of faculty members sourced from different backgrounds, experiences, and specialties work with a class of students would create unique opportunities for developing prototypes and leading the adoption of new practices across the silos of agency, problem set, and academic discipline. A defined period of service would encourage the faculty to maintain a broad network of relationships with other academic institutions, Defense Department sponsors, and industry. In this way, the Digital Service Academy would support the broader ecosystem and not just the institution itself.

Ultimately, both the students and faculty will join the same workforce. We know from our own experience that working relationships with former faculty are very rich and fruitful. The students would form cross-disciplinary networks that intersect with the faculty networks in ways that could provide exponential returns.

Some might argue that limiting the tenure of faculty will impede the development of institutional memory and undermine the ability of faculty to develop long-term projects. There is definitely merit in developing the character of the institution and ensuring that the courses are well-developed. Indeed, there should be a place for long-term research and tenure in academia more broadly. However, we believe that the Digital Service Academy should draw on the best talent from the government, industry, and academia to provide a faculty that is the best in the world. Again, like the Defense Advanced Research Projects Agency model, when a person leaves the Digital Service Academy, that experience becomes a calling card denoting professionalism, knowledge, and experience. Similarly, a member of the Digital Service Academy could return at a later date in a more senior leadership position. To be truly innovative, the academy could build its roster of top talent in the faculty by offering dual appointments to faculty at institutions like Stanford University, Carnegie Mellon University, and the Georgia Institute of Technology. Alternately, imagine having the best minds in AI at Microsoft, Google, Apple, and Facebook spend 10 percent of their time teaching the fundamentals of their latest technology to the next generation of public servants while they are still working on the technology. The best way to have actionable term limits is to place the academy near an existing AI hub, such as Silicon Valley, Washington, D.C., or Austin, Texas. By collocating with existing ecosystems, the faculty can change jobs without having to uproot their families.

How to Fail at Building a Program

We don’t know precisely how to be successful at creating this new type of institution, but we do have some clear ideas about how it might fail. Leading the adoption of AI to solve real-world problems is an inherently interdisciplinary activity. This highlights the challenge of getting faculty to solve problems with others outside their discipline at the speed of relevance. In order to ensure that faculty and their students remain relevant, the academy should not create impediments for faculty to participate in a broad set of conversations — including non-governmental conferences — and publishing in a variety of professional outlets.

Another way to fail at creating a successful Digital Service Academy would be to seal it off from partnerships with industry, academia, and foreign partners with excessive bureaucratic rules. To be successful, the academy would need to be able to create and foster nimble partnerships with non-government research organizations and non-traditional funding sources. The most important thing the academy can do for its students is create an enduring and dynamic ecosystem that spans government, industry, and academia. That support includes identifying meaningful employment opportunities within the government consistent with their education initially, as well as creating a robust alumni network to leverage for the remainder of their careers.

Finally, we caution against creating a so-called “ivory tower,” in which the Digital Service Academy is a standalone organization with permanent faculty measured only against its own metrics. Discomfort

and relevant challenges are key to growth and continued forward movement. This point extends to the enterprise of AI as a whole — it is not an end unto itself. Rather, it is a means to distill knowledge out of data with an ultimate goal of making and implementing better decisions. The best way to avoid an ivory tower is to keep the academy close to practitioners, who are incentivized to deliver results. Keeping this final point in mind is perhaps the most important thing the academy can do.

Conclusion

The United States should adopt the recommendation of the National Security Commission on Artificial Intelligence and establish a Digital Service Academy. It would provide an on-ramp for technically oriented students who might be interested in government service but are not much interested in pursuing a military career. Moreover, it would allow the best talent from government, industry, and academia to develop the workforce and create solutions to many of the most pressing challenges facing the United States. It is also an opportunity to rethink what government service means, in both duration and the ability to work inside and outside the government at the same time.

Many U.S. government agencies have not automated their data collection, developed common analytical tools, or leveraged AI to provide improved services. AI is not an end in itself — the reason to adopt AI is because it is a mature set of technologies that provide a competitive advantage in providing the services our country needs and wants. The Digital Service Academy is one way to get the U.S. government to move faster on a critical issue. When it comes to improving the country's AI capacity, time is of the essence. China is making massive gains in the development and adoption of artificial intelligence across the broad range of governmental activities by integrating those activities in a way that is not seen in the United States. Private industry is outstripping the ability of the government to regulate the adoption of the AI-enabled technologies or deal with the implications of its successes or failures. The need for the Digital Service Academy is incredibly clear.

https://warontherocks.com/2020/09/making-a-u-s-digital-service-academy-work/

Return to Index

RESEARCH:

Navy Researchers Tackling the "Gray Zone" of Sexual Harassment

(WTKR 10 Sept 20)

NORFOLK, Va. - Combating sexual harassment among the ranks has been a focus of military leadership for years, and now they are taking a closer look at what's called "Gray Zone" behavior.

The Navy describes Gray Zone behavior as anything "which falls short of the technical definition of harassment, but most certainly isn't entirely above board."

Researchers at the Naval Postgraduate School have developed a Situational Judgement Test focused on Gray Zone scenarios.

The test is seen as another way to address sexual misconduct and discrimination in the military.

Dr. Gail Thomas is the principal investigator in the research.

"Many academic studies address sexual assault and sexual harassment in the military, but few address the ambiguous behaviors that often precede harassment," she said in a news release.

"What makes this idea so compelling is that instead of looking at incidents after the fact, we are focusing on the 'P' of Sexual Assault Prevention and Response (SAPR) Looking to get in front of potential incidents before they happen," Thomas added.

The research into Gray Zone behavior launched out of an idea from the Navy's Sexual Assault Prevention and Response Office in 2018.

It is focused on Sailors and their immediate supervisors.

"The people who have the most influence on their employees are their first-line supervisors," Thomas explained. "They're the ones who are giving Sailors their fitness reports and who actually establish the immediate work climate."

Through the research, more than 200 examples of 'iffy' situations were curated from the experiences of 63 junior enlisted Sailors and officers.

Those were used to create the Situational Judgement Test.

Participants who took the test were also able to be coached on discerning between what they might do and what they should do in each scenario.

The Navy hopes that the research will result in a better work climate throughout the Fleet.

https://www.wtkr.com/news/military/navy-researchers-tackling-the-gray-zone-of-sexual-harassment

Return to Index

FACULTY:

Twilight of the Human Hacker

(PublicIntegrity.org 13 Sept 20) … Zachary Fryer-Biggs

The Joint Operations Center inside Fort Meade in Maryland is a cathedral to cyber warfare. Part of a 380,000-square-foot, $520 million complex opened in 2018, the office is the nerve center for both the U.S. Cyber Command and the National Security Agency as they do cyber battle. Clusters of civilians and military troops work behind dozens of computer monitors beneath a bank of small chiclet windows dousing the room in light.

Three 20-foot-tall screens are mounted on a wall below the windows. On most days, two of them are spitting out a constant feed from a secretive program known as "Project IKE."

The room looks no different than a standard government auditorium, but IKE represents a radical leap forward.

If the Joint Operations Center is the physical embodiment of a new era in cyber warfare — the art of using computer code to attack and defend targets ranging from tanks to email servers — IKE is the brains. It tracks every keystroke made by the 200 fighters working on computers below the big screens and churns out predictions about the possibility of success on individual cyber missions. It can automatically run strings of programs and adjusts constantly as it absorbs information.

IKE is a far cry from the prior decade of cyber operations, a period of manual combat that involved the most mundane of tools.

The hope for cyber warfare is that it won't merely take control of an enemy's planes and ships but will disable military operations by commandeering the computers that run the machinery, obviating the need for bloodshed. The concept has evolved since the infamous American and Israeli strike against Iran's nuclear program with malware known as Stuxnet, which temporarily paralyzed uranium production starting in 2005.

Before IKE, cyber experts would draw up battle plans on massive whiteboards or human-sized paper sheets taped to walls. They would break up into teams to run individual programs on individual computers and deliver to a central desk slips of paper scrawled with handwritten notes, marking their progress during a campaign.

For an area of combat thought to be futuristic, nearly everything about cyber conflict was decidedly low-tech, with no central planning system and little computerized thinking.

IKE, which started under a different name in 2012 and was rolled out for use in 2018, provides an opportunity to move far faster, replacing humans with artificial intelligence. Computers will be increasingly relied upon to make decisions about how and when the U.S. wages cyber warfare.

This has the potential benefit of radically accelerating attacks and defenses, allowing moves measured in fractions of seconds instead of the comparatively plodding rate of a human hacker. The problem is that systems like IKE, which rely on a form of artificial intelligence called machine

learning, are hard to test, making their moves unpredictable. In an arena of combat in which stray computer code could accidentally shut down the power at a hospital or disrupt an air traffic control system for commercial planes, even an exceedingly smart computer waging war carries risks.

Like nearly everything about such warfare, information about IKE is classified. As even hints about computer code can render attacks driven by that code ineffective, minute details are guarded jealously.

But interviews with people knowledgeable about the programs show that the military is rushing ahead with technologies designed to reduce human influence on cyber war, driven by an arms race between nations desperate to make combat faster.

Using the reams of data at its disposal, IKE can look at a potential attack by U.S. forces and determine the odds of success as a specific percentage. If those odds are high, commanders may decide to let the system proceed without further human intervention, a process not yet in use but quite feasible with current technology.

Ed Cardon, a retired lieutenant general who served as the head of the Army's cyber forces from 2013 to 2016, spent years trying to persuade senior military and White House leaders to use cyber weapons, especially during his tenure running U.S. Cyber Operations against ISIS. He faced stiff opposition because of concerns about the potential of cyberattacks to muddle international relations.

His pitches typically included a lot of guesswork. If Cardon was laying out plans, he'd have to include a slew of unknowns, a couple of maybes and a yes or two when mapping the probability of success. All too often, when Cardon tried to get permission for an operation and had to describe the uncertainty associated with it, the answer would be no.

Cardon, who speaks in a way that forces the listener to lean in, told me that fear of political repercussions was why only a handful of offensive cyber operations were approved during the Obama administration.

But what he saw with IKE could change all that.

"That was what was powerful," Cardon said. "It categorized risk in a way that I could have a pretty good level of confidence."

The Stuxnet episode explains why the U.S. has been hesitant to use cyber weapons. The initial attempt to disrupt Iranian uranium enrichment had worked, blowing up centrifuges in a highly protected nuclear facility, but the code that made the attack successful somehow escaped from that system and started popping up across the internet, revealing America's handiwork to security researchers who discovered the bug in 2010. That led to strict rules governing how and when cyber weapons could be used.

Those rules were laid out in 2013, when President Barack Obama signed a classified order, Presidential Policy Directive 20 that outlined a series of steps, including high-level White House meetings, that would have to take place before U.S. Cyber Command could attack. Military officials quietly complained that the order tied their hands because it was almost impossible to get approval for operations, given the uncertainty around their outcomes.

After the order was in place, the number of global cyberattacks, including those against the U.S., surged. Military defenders had a hard time keeping up; the speed of combat escalated to the point that Pentagon officials feared U.S. networks would be overwhelmed.

In September 2018, President Trump signed off on National Security Policy Memorandum 13, which supplanted Obama's order. The details of the policy remain classified, but sources familiar with it said it gave the secretary of defense the authority to approve certain types of operations without higher approval once the secretary had coordinated with intelligence officials.

The Trump order took effect just before IKE matured from an earlier research program. The order wasn't issued because of IKE, but both were part of a wave of new technologies and policies meant to allow cyberattacks to happen more quickly.

With IKE, commanders will be able to deliver to decision makers one number predicting the likelihood of success and another calculating the risk of collateral damage, such as destroying civilian computer networks that might be connected to a target.

IKE is the model of what cyber warfare will look like, but it's just the beginning. Any automation of such warfare will require huge amounts of data — that IKE will collect — to teach artificial intelligence systems. Other programs in development, such as Harnessing Autonomy for Countering Cyberadversary Systems (HACCS), are designed to give computers the ability to unilaterally shut down cyber threats.

All of these programs are bringing cyber warfare closer to the imagined world of the 1983 film *WarGames*, which envisioned an artificial intelligence system waging nuclear war after a glitch makes it unable to decipher the difference between a game and reality.

IKE hasn't been turned into a fully autonomous cyber engine, and there's no chance nuclear weapons would ever be added to its arsenal of hacking tools, but it's laying the groundwork for computers to take over more of the decision making for cyber combat. U.S. commanders have had a persistent fear of falling behind rivals like China and Russia, both of which are developing AI cyber weapons.

While the growing autonomous cyber capabilities are largely untested, there are no legal barriers to their deployment.

What worries some experts, however, is that artificial intelligence systems don't always act predictably, and glitches could put lives at risk. The computer "brains" making decisions also don't fret about collateral damage: If allowing U.S. troops to be killed would give the system a slight advantage, the computer would let those troops die.

"The machine is perfectly happy to sacrifice hands to win," Cardon said.

As these increasingly autonomous systems become more capable, top White House officials must decide whether they're willing to give AI computers control of America's cyber arsenal even if they don't understand the computers' decision making.

"The nice thing about machine learning systems is that they often spit out numbers," said Ben Buchanan, a professor of cybersecurity and foreign policy at Georgetown University and author of *The Hacker and the State*. "The dangerous thing is that those numbers aren't always right. It's tempting to assume that, just because something came from a computer, it's rigorous and accurate."

PLAN X: A NEW TYPE OF CYBERWARFARE

The basics of cyber operations are fairly simple. Experts, whether working on offense or defense, have to figure out which computers or other devices are on a network, whether they have any weaknesses in their defenses. Then hackers exploit those weaknesses to take control of a system, or, if they're playing defense, fix the vulnerability.

Having gained control of a system, an attacker can pretty much do what he or she wants. For intelligence agencies, that usually means meticulously monitoring the network to learn about the adversary. The rest of the time cyber operators are looking to disrupt the system, destroying or replacing data to undermine an opponent's ability to work.

Thus far, full-scale cyberwar hasn't broken out, with combat confined to skirmishes between countries that try to deny responsibility for strikes. One of the benefits of using computers is that countries relay the code that runs their attacks through multiple networks, making it harder to track the source of the attack. But the dozen or so countries with advanced cyber capabilities have been busy hacking everything from power plants to fighter jet manufacturers, thus far focused on stealing information.

For the first era of cyber warfare, which picked up steam at the beginning of the millennium, the processes of attacking or defending meant a manual series of steps. The Pentagon was busy purchasing one-off tools from tech companies offering solutions to track all the computers in a network and find weaknesses in their code. That meant one expert would sit at a computer using a program such as Endgame, while another, at a different computer, might use a piece of software such as Splunk. Everything moved slowly.

"You could be sitting right next to each other, and the person right next to them would not have any idea what the other was doing," John Bushman, a former U.S. Army Cyber Command official told me.

To create a battle plan, experts would have to step away from their computers, draw up strategies on whiteboards or sheets of paper, return to their stations and engage in a series of sequenced moves to win the battle. By 2012, the military had tired of this old-school approach. It was tedious work, given that so much coordination had to take place away from keyboards. Almost every cyber unit could report at least one instance of a bleary-eyed hacker accidentally leaning against a whiteboard and wiping out a battle plan.

The Pentagon tasked its research arm, the Defense Advanced Research Projects Agency (DARPA), famous for inventing the internet and the computer mouse, with trying to come up with a better way to run cyber wars.

Early systems helped simplify what the troops were doing, but they were still facing massive hurdles, mainly because there are fewer than 7,000 experts at U.S. Cyber Command trying to defend countless systems.

DARPA's answer was to contact software companies for a new program officially called Foundational Cyberwarfare, but affectionately nicknamed "Plan X."

In its announcement of Plan X in 2012, DARPA made clear that cyber warfare had to get beyond the "manual" way of waging war, which, it said, "fails to address a fundamental principle of cyberspace: that it operates at machine speed, not human speed."

Nearly a decade later, Plan X has morphed into Project IKE. The Pentagon will spend $27 million on it this year, and plans to spend $30.6 million next year.

The original work on Plan X looked nothing like the team-management and predictive engine that IKE would become. It was much closer to the interactive screens and neon lighting of the film *Minority Report*, focusing on displays of data showing what was happening on computer networks.

"The rule for the first couple of years was, if we end this program with a keyboard and a mouse as the interface to our data, we have failed," Jeff Karrels, who runs the division of the contracting firm Two Six Labs that built much of Plan X, told me in an interview. Researchers toyed with having hand gestures control the system along with three-dimensional holographic projections.

Instead of the old sand tables with little models of troops and tanks, the new visual system would be fed by a constant stream of data on the work of U.S. cyber troops. Two Six hired game developers to work on the interaction between humans and the complex models they'd be presented with.

Eventually, enthusiasm for the virtual-reality version of battle waned. Those working on the program began engineering a new way to combine different cyber software the Pentagon had already bought so it could all work on the same computers. That meant helping to create automated tools that could run several programs in quick succession, speeding up operations by reeling off a string of steps in a campaign.

The shift resulted in a system that wasn't focused on the big picture — planning and running wars — as had been one of the original goals of the program. Rather, the aim was to simplify some smaller steps.

That was until 2015 arrived.

Up until that point Cardon, the retired lieutenant general, had been keeping an eye on the program and feared the experts were missing an opportunity.

Frank Pound, who managed Plan X for DARPA, remembered sitting in a meeting that year with Cardon to discuss the progress that had been made. U.S. Army Cyber Command, the group that Cardon commanded, had become closely involved with the program early in its development although it was a DARPA project.

"We were trying to build a system that would allow them to fight back," Pound recalled in a 2018 interview, describing the pivot to combined software.

Cardon had a different message.

"Oh, it's much more than that," he said. Cardon nearly reached across the table and grabbed Pound by the lapels. He wanted Pound to see Plan X's full potential. It could help coordinate all cyber operations, while constantly chewing through information on Defense Department networks to find new vulnerabilities and ferret out attackers. It could use all of that data to help make decisions on which attacks by U.S. forces might work, and when they should be used.

That vision, closer to the all-consuming platform that DARPA had originally described in 2012, would suddenly seem very different once another DARPA program took center stage in the summer of 2016.

Sure, Plan X might be able to help digest all the data about computer networks, but what if it could feed a system smart enough to wage its own cyber war?

MACHINE LEARNING

At first glance, the Mayhem Cyber Reasoning System looks like an engorged gaming computer, a black rectangular box about 7 feet tall with neon lights and a glass side revealing row after row of processors. When the National Museum of American History decided to display the machine in 2017, it sat in a hallway near an exhibit showing off some of the nation's greatest inventions, including a model of the original prototype that would lead to Morse code.

The glowing Mayhem box might not seem worthy of comparison to that earth-shattering invention, but a museum curator and a slew of experts with DARPA thought it might herald a seismic shift in cyber warfare.

Mayhem was the victor in a 2016 DARPA competition, besting a half-dozen competitors in a hacking competition. What made this competition different from previous ones was that Mayhem had no human directing its actions. Once challenged, it had to make its own decisions about when and how to attack competitors and how to defend its own programs, developing strategy for how to win a contained cyber war that played out in five-minute rounds over the course of a day.

Curator Arthur Daemmrich walked a group of DARPA officials through the museum for the exhibit's grand opening. The officials told Daemmrich that they felt an obligation to develop new cyber systems because of the organization's ties to the birth of the internet.

"DARPA at some level feels a responsibility to have the internet function in a secure fashion and not be rendered useless by hacking," he said.

Finding a way to automate cybersecurity is the kind of complex problem DARPA likes to grapple with. The biggest projects launched by the agency tend to come in the form of what it calls "Grand Challenges," some of which can be bit too grand. A 2004 competition testing autonomous vehicles had 15 entrants vying for a $1 million prize. None managed to complete the 150-mile driving course, and the winner managed only 7.3 miles.

DARPA viewed this not as a failure but as a sign it was helping to advance the technology in the field. A 2005 competition had nearly two dozen entrants, five of whom managed to complete the 132-mile course. A machine developed by a team from Stanford University recorded the fastest time and won its handlers a $2 million prize.

In 2013, DARPA announced the Cyber Grand Challenge, the competition Mayhem would claim. The winning team would get $2 million if it won a capture-the-flag contest modeled on the one held every summer in Las Vegas at the DefCon hacking convention. It's the gold standard for such events, pitting teams of humans against each other to attack and defend custom-built computer networks while scoring points based on how successfully they can meddle with their opponents' computers while protecting their own. It's a microcosm of the kind of combat hackers encounter in the real world.

The very idea for the Cyber Grand Challenge had come out of the DefCon competition. Mike Walker, the DARPA program manager who would run the Cyber Grand Challenge, had spent years competing in the DefCon capture-the-flag competitions and noticed an increased use of automated tools. These were narrow in scope, limited to what hackers call "fuzzing" — a brute-force effort to throw challenges at a piece of software until something breaks. When it does, hackers reverse-engineer the problem to see if they can use it to sneak into a system.

Walker, who declined to be interviewed for this story through his current employer, Microsoft, admired the progress computer systems like IBM's Watson and Deep Mind's AlphaGo had made in playing games like Chess and Go, according to former colleague **Chris Eagle, a professor at the Naval Postgraduate School in Monterey, Calif.**

The key question Walker kept asking was whether a computer could play capture the flag the way Watson played chess.

Machine learning is what makes Watson work. Simply put, it is given a large pool of data to pick through. Different techniques are used for the computer to learn lessons, but in general it finds patterns and uses those patterns to make predictions. This type of learning doesn't yield the kind of near-human personality present in HAL 9000, the ill-intentioned computer in "2001: A Space Odyssey," but it does allow a machine to arrive at its own conclusions independent of humans. And because it can analyze far more data than a human can in a short period of time, the predictions can evaluate a lot more detail.

The problem with machine learning is that computers can't explain how they come up with the answers they do, meaning users have to trust that the conclusions are sound.

"Machine learning is often like a smart but lazy eighth grader taking a math test: It's great at getting the right answer, but often pretty bad at showing its work," Buchanan, the Georgetown professor, told me.

Mayhem used automation to allow the machine to make tactical decisions on when to break into an opponent's system, or when to try to fix weaknesses in its own defenses, to an extent far beyond what the fuzzing hackers had used before.

Once the Cyber Grand Challenge competition got underway in August 2016, Mayhem began to malfunction. The system was supposed to constantly turn out new attacks and fixes to its defenses but went quiet.

"That's when we realized that something was misbehaving very badly," Alex Rebert, the leader of the Mayhem team, said. "It was rough, it was very stressful. We had just spent two years of our lives working on this, and then the day of the competition it misbehaves."

The team members were deflated. They tried to get the other competitors to let them restart Mayhem, hoping that would flush out the bugs, but were turned down. Then something clicked. Mayhem sprang back to life and won.

One problem with systems that rely on machine learning is that it's difficult to test them, and they can be prone to cheating. In one experiment, a computer taught to play Tetris concluded the best way to achieve its mission — not losing — was simply to pause the game.

Whichever tools military researchers develop using AI, it will be hard to gauge how they might work in combat. It's still not clear how to test machine-learning systems that are constantly adjusting their conclusions based on new data.

Many experts in the cyber field had made the trip to Las Vegas to see the Cyber Grand Challenge, including Lieutenant General Cardon, and their imaginations were sparked.

Most in the audience didn't see gremlins at work in Mayhem and didn't know that even this apparently sophisticated combatant still had major bugs. They simply saw an autonomous system succeeding in cyber combat.

"When I saw that, I'm like, 'Oh my gosh, if you put that together with Plan X, this is how you would conduct operations,'" Cardon said.

A 'NEW ARMS RACE'

Frank Pound, the head of DARPA's Plan X effort, gave me a demonstration of the system during a conference in September 2018.

Spurred by Cardon's insistence that the program could become the platform for all U.S. military cyber warfare, Plan X had morphed into a broader management tool for cyber operations.

Gone were the high-tech digital sand tables. Left were a pair of screens, with charts listing the people on each cyber team and who should report to whom. Modules on the side coughed up a stream of data showing what was happening on the network. You could click through to find out more about the hackers behind each dot, learning about their skill sets and past mission successes. The data on the screen was a mock-up, with the actual details classified.

“Think of it as a full-spectrum cyber operations platform specifically designed for military operations with all that rigor and discipline,” Pound told me.

Pound was a couple of months from leaving his post at DARPA, cycling out after several years, as most program managers do.

The DARPA program itself had evolved, but the broad outlines of its work were still public, and I was standing in an exhibition hall for a celebration of DARPA’s 60th birthday, and a demonstration on how commanders might use the system.

The Trump directive making it easier to launch cyberattacks was announced only a few weeks after Pound and I spoke.

And soon after that, control of Plan X would be snatched by one of the more secretive wings of the Pentagon’s research structure.

Ash Carter, then deputy secretary of defense, had created the Strategic Capabilities Office in 2012 to take on the mission of converting promising technologies to real battlefield tools. While DARPA still had a mission of fiddling with concepts that were largely theoretical, the SCO was supposed to make sure all of this work quickly translated to combat.

When SCO took over Plan X in December 2018, one of the first things it did was change the program’s name. Plan X had too much baggage tied to its first iteration as an elaborate and futuristic battle visualization tool. Instead the office renamed it Project IKE. Those who worked on the program insist that IKE doesn’t stand for anything, but rather was meant as a cheery new moniker, a play on the “I like Ike” slogan that swept Gen. Dwight Eisenhower into the White House.

SCO had an important message for the program’s main contractor, Two Six Labs: Make sure the system was using machine learning to make more predictions, not just keep track of hacking teams. Having seen what Mayhem had been able to pull off at the Cyber Grand Challenge, Pentagon leaders were convinced that more automation and artificial intelligence could be pushed into its new cyberwarfare star. The ability to calculate a single number measuring the likelihood of a mission’s success became key, as did using computer thinking to help figure out how to structure teams of cyber experts.

SCO also began to look at how IKE could use machine learning to develop information about targets for potential attacks. The idea was to let the computers pull information from different sources to create a clearer picture about what a target looked like.

That focus on artificial intelligence has driven constant improvements on IKE ever since. Every three weeks an updated version of the system is finished and sent to U.S. Cyber Command.

Once IKE left DARPA, it was quickly hidden behind a thick veil of Pentagon classification. The Defense Department’s annual budget documents sent to Congress name the program and lay out the amount of money sought — $30.6 million for 2021 — but all other details have been withheld.

Several sources, however, told me Project IKE is on the cusp of being able to perform many of its functions without human intervention. The big question is whether Pentagon and White House officials will let it.

Congress, thus far, hasn’t stepped in to establish limits on how the military can use its blossoming cyber arsenal. The U.S. Cyberspace Solarium Commission, chaired by Sen. Angus King, I-Maine, and Rep. Mike Gallagher, R-Wis., studied a range of issues involving cybersecurity and expressed concern about the rise of artificial intelligence. The commission’s final report, released in March, found that AI could lead to a “new arms race” but didn’t suggest any form of regulation.

Without it, the Pentagon has pressed on, developing the most advanced tools it can.

A newer DARPA program, known as Harnessing Autonomy for Countering Cyberadversary Systems, is trying to develop systems that can hunt on their own for certain types of attackers, mainly botnets that flood victims with traffic from numerous computers. It’s the kind of program that could be plugged into IKE to automate more cyber combat.

Karrels's company, Two Six Labs, is also working on the HACCS program, and says the big question is whether U.S. Cyber Command would unleash it. Even if the technology is capable, without rules about when it could be used, it's unclear if it would be deployed.

From a technology standpoint, the hard part is done, and the software is already capable of planning and launching its own attacks if cyber experts let it. That could make massive botnet attacks, the type that often disable bank websites and others, a thing of the past. It's also largely unproven technology that could start shutting down and damaging critical computer networks accidentally.

Either way, the technology is ready.

"We are danger close on all of that becoming a reality," Karrels said.

https://publicintegrity.org/national-security/future-of-warfare/scary-fast/twilight-of-the-human-hacker-cyberwarfare/

Return to Index

ALUMNI:

Arab American Women in Government – A Conversation

(The Media Line 8 Sept 20)

Date and time: Thursday, September 17, 2020, 7 to 8 pm Eastern Daylight Time (UTC-4)

Join Jennifer Atala of Inara Strategies for an off-the-record conversation with four incredible Arab-American women serving in government.

Arab Americans are a lesser-known community, despite the high proportion our countries of origin take up on news cycles. We are Christian, we are Muslim. We span the gender identification spectrum. We are athletes, we are academics. We are artists, and we are business-people. We are first-generation immigrants and refugees, and we have been Americans for many generations. We are cultural diplomacy leaders, and we are experts at counter-terrorism

As all eyes are on the 2020 presidential election, we thought it would be an important moment for our voices to be included in the conversation of what it means to SERVE. To serve our American government, together, through the ups and downs of elections cycles, during leadership changes as Administrations change political parties, as experts in our fields, as women, as proud Arab Americans

Nabeela Barbari

Nabeela Barbari is the Deputy Associate Director of Strategy and Resources within the Cybersecurity Division at the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). In this role, she leads a team that develops strategy and oversees the budget and implementation of CISA's mission to strengthen the security and resilience of the cybersecurity ecosystem.

Prior to this, Nabeela was the Acting Associate Director of Plans and Programs at the National Risk Management Center at DHS/CISA. From 2016-2018 was a Senior Policy Advisor at the DHS Office for Civil Rights and Civil Liberties providing expertise to government officials and leading public engagements on national security policy, countering violent extremism, and civil rights matters. Nabeela also spent 8 years at the DHS Office of Infrastructure Protection in a variety of roles related to counterterrorism and public/private partnerships. Nabeela holds two Masters Degrees – **one from the US Naval Postgraduate School Center for Homeland Security & Defense** and the other from George Mason University, as well as a Bachelor's Degree from Virginia Commonwealth University.

Arab country of origin: Palestine

https://themedialine.org/mideast-streets/arab-american-women-in-government-a-conversation/

Return to Index

Leadership Through Homegrown Values

(Army.mil 9 Sept 20) … Ellen Summey

COMMAND/ORGANIZATION: Product Manager Heavy Tactical Vehicles, Project Manager Transportation Systems, Program Executive Office for Combat Support and Combat Service Support

TITLE: Program officer

ACQUISITION CAREER FIELD: Program management

YEARS OF SERVICE IN WORKFORCE: 18 years 9 months

MILITARY OR CIVILIAN: Civilian

DAWIA CERTIFICATIONS: Level III in program management and in engineering

EDUCATION: **M.S. in program management, Naval Postgraduate School**; B.S. in mechanical engineering, Lawrence Technological University

AWARDS: Commander's Award for Civilian Service, June 2014

HOMETOWN: Erie, Pennsylvania

DANIEL C. JESKA

Treat people with respect. Be accountable. Communicate clearly. Never burn bridges. Dan Jeska abides by a few basic rules he learned while growing up in rural Pennsylvania. As a boy, he developed a love of the outdoors, and he spent nearly every waking moment roaming the rolling hills outside his back door. In keeping with this very bucolic scene, his first job was on a dairy farm. "Looking back now, I really appreciate that simplicity," he said. "When the boss told me to move hay bales from one spot to another, that was all I needed to know."

To say that things have become more complex since that time might be an understatement. Jeska is now a program officer for Product Manager (PM) Heavy Tactical Vehicles within the Program Executive Office for Combat Support and Combat Service Support (PEO CS&CSS). Along with two assistant program managers and their integrated product teams, the PM is responsible for the Army's Heavy Expanded Mobility Tactical Truck, Palletized Load System trailer, Heavy Dump Truck and distribution enablers. The PM team is also in the early phase of a joint U.S. and United Kingdom project to develop a next-generation heavy tactical vehicle system. Jeska has moved up from hay bales to huge armored vehicles, but he's still the same soul underneath the titles and technicalities.

After moving to Michigan with his family, Jeska completed his bachelor's degree in mechanical engineering and went to work for large companies in the automotive industry. "At my last industry job, we made instrument clusters and heads-up displays for cars," he said. "I worked with some really great people there." But he became frustrated by the high rate of turnover and the poor quality of life in the industry. "The turnover rate at one of my employers was over 20 percent each year. It was just the nature of the industry," he said. "I was getting burned out."

Around that time, he went out to lunch with a friend from college who encouraged him to consider becoming an Army civilian. "He told me he had a better quality of life at TARDEC [the U.S. Army Tank Automotive Research, Development and Engineering Center, now the U.S. Army Combat Capabilities Development Command Ground Vehicle Systems Center]," which was just around the corner in Warren, Michigan. So Jeska went to a job fair and started applying. When he eventually interviewed for a job, he had one very important question for the boss. "As we walked around the office and met some of the other staff, I asked how long they had been working there." He was looking for an employer that would value and invest in its workforce—and after that day, he was sold.

Jeska said his experiences as an Army civilian "couldn't be more different" than his time working in the auto industry. "The Army invests in its employees and develops them," he said. "Leaders want their subordinates to succeed and be promoted to their fullest potential." And he has never been left wanting for opportunity in the acquisition community. "There is no need to worry about stagnating on a single program for your entire career," he said. Jeska said there is ample room for growth, whether by moving to a new program or exploring development programs within the Army acquisition community.

Since entering the acquisition workforce nearly 20 years ago, he has seen a lot of changes. So, what stands out as the biggest? “What comes to mind is the approachability of our leadership,” he said. “I’ve seen a huge improvement in communication over the years.” Communication has been emphasized by leaders across the Army, and has also become a priority at PEO CS&CSS. For example, Jeska takes part in quarterly off-site meetings with his counterparts and other staff from within Project Manager Transportation Systems. “We are located in different offices, so we may not really interact, otherwise,” he said. “We give it our full attention, away from our regular duties and distractions, and really learn from each other and share ideas.”

The importance of communication and building professional relationships is personal for Jeska, as well. It’s a lesson that goes back to his early years in Pennsylvania, when he learned the value of simplicity. “No matter who you are speaking with, never assume you know more than they do,” he said. “Ask questions to make sure you understand and work to find compromise. Never burn bridges.” He told a story about working through a problem with a colleague on a truck project a decade ago. Because he had established a good rapport with that individual, the two were able to defuse a very tense situation years later. “Tensions were high and very senior leaders were involved,” he recalled. “When I heard a familiar voice, I remembered our experience from many years back. In a matter of 10 minutes, he and I had found a path to resolution.”

That lesson is all the more relevant today, in light of the ongoing COVID-19 pandemic and the associated challenges with sudden and prolonged remote work. Jeska said he sometimes sees telework creating inefficiencies for his team. “Things that would normally take five minutes are now more difficult,” he said. Before, he could pick up a paper, walk to an engineer’s office, and sketch out a solution in real time. “Now, I find myself making a few slides and adding some big arrows or illustrations to make things really clear,” he said. “Then we get on the phone and talk through it.” It may take a little longer these days, but effective communication is still a priority to him.

If he were crowned “King of Acquisition” for a day? “I would love to power down some of our decision-making to lower levels, to free up our PEOs and senior leaders to focus on higher-level decisions and steering the organization,” rather than being burdened with the minutiae of day-to-day business. “By empowering our people and clearly communicating their left and right limits, we could see faster decisions on routine matters.” Let them move the bales of hay, in other words, so the farmer can take care of bigger concerns.

“Faces of the Force” is an online series highlighting members of the Army Acquisition Workforce through the power of individual stories. Profiles are produced by the U.S. Army Acquisition Support Center Communication and Support Branch, working closely with public affairs officers to feature Soldiers and civilians serving in various AL&T disciplines.

https://www.army.mil/article/238878/leadership_through_homegrown_values

Return to Index