2022

# Faces of NPS: Lt. Col. Sam Gray

Gray, Sam

Naval Postgraduate School, Monterey California

http://hdl.handle.net/10945/71192

# Faces of NPS

Spotlighting the students, faculty, staff and alumni of our Nation's premier defense education and research institution.

## Lt. Col. Sam Gray

MS IN OPERATIONS RESEARCH '17,
CYBERSECURITY FUNDAMENTALS CERTIFICATE '20
MARINE CORPS SERVICE LIAISON, OSD STRATEGIC CAPABILITIES OFFICE

Lt. Col. Sam Gray:

Lt. Col. Sam Gray is the Marine Corps Service Liaison to the Office of the Secretary of Defense Strategic Capabilities Office (SCO) where he identifies SCO technologies being developed that will support the Marine Corps and Force Design 2030. Additionally, he serves as a program manager at SCO focused on technologies dealing with machine learning, artificial intelligence, robotics, autonomy and digital engineering. His efforts include identifying and integrating emerging commercial digital technologies into DOD capabilities, developing innovative methodologies to conduct smarter sustainment of legacy DOD platforms, and prototyping scalable modeling and simulation environments to support operations. Gray also served as a subject matter expert to the National Security Commission on AI.

Gray was commissioned into the U.S. Marine Corps in 2005, serving as a logistician in the Fleet Marine Force. He has served at the tactical, operational and strategic levels to include four operational deployments in Iraq, Afghanistan, and in support of a Special Purpose Marine Air Ground Task Force. He holds an MS in Operations

Research, with a focus on data science, and a graduate certificate in cybersecurity from the Naval Postgraduate School. He also has multiple Harvard Kennedy School Executive Education certificates in public policy, cybersecurity and artificial intelligence.

*"Industry, academia, and the government have to partner closely to keep a technological edge. Gone are the days of the government driving state of the art innovation – we have to partner... The battlefield is becoming more and more digital – that is technology plain and simple. To have an edge on the battlefield you have to have an edge in technology."*

**How did your time at NPS and the OR program impact your career and equip you to contribute to U.S. national security in your follow-on positions? In what ways did it shape your understanding of digital technologies and how you think about application in current and future battlespaces?**

NPS and the Operations Research program made a significant impact on my career path and prepared me to handle the unique assignment that followed. First, I was able to unlock my inner "nerd," enabling an analytical way of thinking and decision making. Second, it provided me with the foundational knowledge to have in-depth technical conversations with academia and industry. This skill, coupled with my operational experience allowed me to be a translation layer from Nerd to Operational User and back. Finally, NPS gave me the confidence to tackle technical areas where I was not formally trained. The educational methods learned let me teach myself the necessary technical information for areas outside of Operations Research. This approach to lifelong learning allows me to stay current with various technologies and put an operational spin on basic research ideas. This will be critical given the ever-changing digital battlefield. As everything becomes software defined, it is critical to have a cadre of technologically savvy uniformed personnel, focused on delivering state-of-the-art capabilities to the Fleet.

**The DOD Strategic Capabilities Office develops innovative ways to address operational challenges with emerging technologies. How does the SCO work with the services and research laboratories to identify challenges and to test and iterate these technologies? What value does (or could) NPS — where operational students, researchers and industry partners work side by side — add to the process?**

SCO is closely aligned with the Services and research labs. The office is more R&D focused vice pure S&T, which is where the labs tend to focus. This allows SCO to take basic research or low TRL technologies being tested and scale them to meet an operational need or mission. However, being technology-demonstration focused means there is less attention paid to the analysis of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P). This necessitates a partnership with the services to ensure there is a "Big R" Requirement, so the technology avoids the proverbial "Valley of Death" and becomes a sustainable long-term program. SCO partners with services to demonstrate new technologies and give Soldiers, Sailors, Airmen, Marines and Guardians the ability to test and break the technologies by putting hands on. Iterating on technology with feedback from end users is the best way to deliver a capability the services actually want and need.

NPS sits at a unique nexus where it can be mutually beneficial to the DOD Strategic Capabilities Office and the services. By generating and analyzing various concepts of employment of a specific technology and how it fits into a specific scenario, SCO can gain quantitative analysis of the capability informing future resource/funding decisions while the services can use the same data to help justify funding in the Program Objective Memorandum (POM). NPS is one of very few mixing bowls of vast operational experience and technology in a common location.

**Private industry outpaces government development of various digital technologies in many ways. In your role as a SCO program manager, how do you and your colleagues work with private industry to rapidly equip the DOD and our warfighters with the best and most relevant technologies? How does developing our technological edge strengthen our national security?**

Industry engagement is critical to ensure SCO is delivering the most relevant and cutting-edge technologies being developed. For me, this involves the traditional defense companies along with expanding out into industry and academia as far as possible. To this end, I attend the Consumer Electronics Show (CES) to see where technology is heading. As a Program Manager, I don't necessarily want the tech that is already in market, I want the cutting-edge stuff being developed behind closed doors with Independent Research & Development (IRAD). CES offers a little peek behind that door. To deliver at a speed that matters I want the ability to run parallel with a company's research, so that when the technology is ready for "go to market" there is already a Requirement, interested transition partner, and concept of operations. Industry, academia, and the government have to partner closely to keep a technological edge. Gone are the days of the government driving state of the art innovation – we have to partner. As previously mentioned, the battlefield is becoming more and more digital – that is technology plain and simple. To have an edge on the battlefield you have to have an edge in technology. Perhaps this means adjusting the old shoot, move, and communicate adage to be shoot, move, communicate, and code.

**Our daily life, economic vitality and national security depend on a stable, safe and resilient cyberspace. There are many advances in technology that could help protect against cyber threats and mitigate vulnerabilities. In what ways does your work with various digital technologies, such as Artificial Intelligence, autonomous systems and cloud computing, support cyber defense capabilities for our military and our nation? How can these digital technologies support offensive cyber operations?**

Bruce Schneier discusses some of this in his book *Click Here to Kill Everybody*. The premise is that everything is a computer, and therefore vulnerable. This is true in our everyday lives from coffee pots to cars, there are new threat vectors being added to the "network" daily. The same is true on the modern battlefield. As we interconnect everything, we create vulnerabilities and data that is too much for a human (or group of humans) to process. This is where things like machine learning, AI if you want to call it that, autonomous systems, and the cloud support the human operators. As the amount of data increases exponentially at machine speed, the triage of the information and identification of anomalies must be augmented with things like machine learning and automation. When potentially being attacked at machine speed, you have to defend at machine speed. A good strategy is to couple these exquisite defenses with simple things like proper cyber hygiene and digital awareness to serve as a first line of defense. Artificial General Intelligence doesn't exist, so machines do what they are programmed to do, meaning humans are still our greatest vulnerability with respect to cyber. From an offensive cyber perspective, a solid approach is to "Red Team" yourself and see if any of the ML / autonomous agents generated can exploit your own vulnerabilities. Identifying less robust areas in one network may offer useful insights into someone else's network.

**On October 7, the current administration announced a new export controls policy on AI and semiconductor technologies to China. The policy signals the belief in the transformative potential of AI and its national security implications, but it won't stop China from competing and trying to gain a technological advantage using their "military-civil fusion" strategy. Based on your experiences, what needs to change in**

**the U.S. defense acquisition and adoption process to ensure we maintain a competitive advantage in future fights?**

There is a lot to unpack in this question. This would be a good thesis topic. The competition is real. Digital technologies, including AI, have and will have a significant impact on national security. A trusted foundry and supply chain, where we can unleash brilliant engineers to push the bounds of developing the next generation of semiconductors, are critical. The pace at which digital technology changes is measured in weeks and months, not years and decades. With all those being assumptions (I would argue facts), I have a couple personal opinions (not those of SCO, OSD, government, or the Marine Corps) for ways to test a slightly different approach to digital technology acquisition.

The Contract Data Requirement List (CDRL) or Milestone Deliverables for software technologies MUST be written to provide maximum freedom to both the government and performer. For hardware systems these deliverable or minimum requirements are more easily measured – must go mach X, range of Y, etc. In software, if developing correctly, you are rapidly building, testing and deploying things into production. This means Contract / Agreements officers have to become comfortable accepting more flexibility, and therefore risk. The potential return on the risk acceptance is huge – where if we treat software like hardware of old, we will end up with old, antiquated systems. Some mechanism exists already to spread the risk. Cost plus and T&M contracts alleviate putting all the risk on the contractor, which can potentially increase flexibility.

There needs to be a mechanism to identify new software / digital technology and rapidly test the efficacy of the tech. When building out a prototype to see if there is transferability from an industry use to a government use, we cannot afford to move at the speed of the traditional acquisition system.

There needs to be a better method of dealing with the "as a Service" (AAS) model. Many digital technologies are AAS, which creates issues with how the DOD budgets and pays for things. There is precedence for this type of spending (facilities, electricity, etc.) – we have to codify it for software.

There needs to be a mechanism to ensure that funds and contract vehicles exist to rapidly acquire new technologies that emerge from industry. This means exempting funds from the traditional obligation and expenditure metrics, which exist because of the old, antiquated acquisition process. If industry unveiled a teleporter that could safely move a platoon anywhere in the world in minutes – it would take years (without Senior Leader influence) to acquire into a program of record. The current process would be the same for new software.

Not all is lost, as there are many efforts underway to improve these processes. The Software Acquisition and Practices (SWAP) Study released by the Defense Innovation Board is helping push the ship in the correct direction.

**Is there anything you can share about current projects or priorities of SCO? What technologies do you personally think will have the most transformative impact on national security strategy over the next several years?**

I think it will be a combination of advances in modeling and simulation paired with machine learning / AI. Think about the work being done at DeepMind with their Alpha series (Go, Zero, Fold, etc.) and the impact that has had on shedding light on the power of AI. Pair that with a Mod/Sim environment that is capable of integrating models (digital twins, economic models, behavior and social models) and data from a vast array of sources – with varying fidelity to build optionality and capability. To impact national security, you have to be able to determine the entanglement between the various instruments of national power internally and externally to our government. What is the impact of sanctions here, embargos there, a carrier strike group transiting a "contested" waterway, or a CODEL visiting specific regions? All those actions generate second, third, etc. order effects. Continued advances in computing (GPUs, TPUs, etc.) enable this integration, while also making some of the agents autonomous. Eventually I believe it will be possible to pit machine vs. machine in a digital environment – ideally generating a "Move 37" for the government. This may seem far off, but I believe it to be closer than some may think.

https://www.npsfoundation.org/faces-of-nps/sam-gray