

HACK THE MACHINE UNMANNED

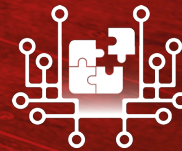
The United States Navy is bringing velocity to the development and fielding of unmanned systems at scale. Join us as the U.S. Navy stands up an **Unmanned Task Force** to solve key operational problems in new ways. **HACKtheMACHINE Unmanned** is the first in a series of public facing technology challenges that accelerates discovery and teambuilding between the Navy, Industry and Academia for the creation of high-end autonomous capabilities

ANSWER THE CALL!

We are looking for people from all walks of life to help the Navy solve its foremost digital challenges. The Office of Naval Research is leading the search for creative, bright, team-building collaborators and learners who know how to hustle and get things done. HACKtheMACHINE is your opportunity to solve problems, win prize money, earn contracts and be part of this dynamic group.

16-19 NOV 2021

 HACKtheMACHINE.ai



CHOOSE YOUR CHALLENGE

HACKtheMACHINE Unmanned offers three challenge tracks to appeal to a broad range of talents and skill sets.

Track 1: Maritime Cyber

HACK THE PILOT

Do your part to make the Navy's next generation unmanned drone swarm autopilot systems ready for prime time by testing their security in this bug bounty contest!

Track 2: Data Science

DETECTIVE BOT

Help bring useful, battle-tested machine learning and artificial intelligence tools to the Navy by developing methods to sort good data from dangerous data in degraded environments.

Track 3: Digital Engineering

TOP MODEL

Show the Navy how to create model-based definitions of requirements for wide-area search that can be tested against real system models in unmanned mission simulations!

Track 1: Maritime Cyber

HACK THE PILOT

In unmanned systems, autopilot isn't just an option, it's the default. Considering how many autopilots are running in a swarm mission, how secure are they? Could an autopilot be hacked and used to gain access to the other autonomous systems, manned vessels, or even command and control? In this challenge, teams will put their skills to the test in a bug bounty. Leveraging afloat, undersea, and drone autopilot systems, teams will win cash for uncovering vulnerabilities in autopilot systems.

AND THERE'S MORE!

Behind the scenes a team of government stakeholders is convening to create an even bigger Track 1 challenge for the next installment of HACKtheMACHINE Unmanned. Right now, specs are being defined for the next gen unmanned cybersecurity infrastructure, networking, access, and data transfer architecture the Navy may deploy. Innovators up for the challenge will have the chance to design implementations and pen-test to find gaps in cybersecurity architectures under consideration.

Join us now to be among the first to know what is next at HACKtheMACHINE.ai!

Track 2: Data Science

DETECTIVE BOT

The Navy is pursuing Machine Learning and Artificial Intelligence (ML/AI) tools that can distinguish benign from malicious code. While some techniques have shown great promise in benign/malicious selection, the compute load of these techniques requires many GPUs and CPUs, running dedicated jobs in a data center or in the Cloud. Can autonomous systems do as well? Can benign and malicious code detection run at the edge in an unmanned swarm of afloat platforms where limited compute environments – servers, CPU, storage, power – all must exist in a few racks or small chassis far from shore and disconnected from the Cloud.

We are providing a dataset with thousands of malicious and benign code samples to see who can take inefficient AI/ML techniques developed with 'unlimited' resources ashore and adapt them to efficient and effective cyber solutions on smaller afloat and autonomous platforms.

Track 3: Digital Engineering

TOP MODEL

Imagine the possibility of hundreds of drone companies and thousands of good ideas aligned to provide the Navy with the fighting edge it needs in unmanned swarms. In the coming months there will be several opportunities to get hardware systems out to sea and evaluated by the Navy, but we do not have a model-based way to define its needs for industry or a common pattern for simulating the effectiveness of a new technology before a live event. Innovators are wanted to help build a model-based systems engineering approach to this problem.

We are providing a description of the requirements for wide area search in the southern hemisphere in search of a model-based definition of the requirement. Next, two model-based examples of unmanned search systems will be developed for testing against the requirements model. Who can show the Navy how to run a simulation of example systems that demonstrate their effectiveness on the desired search criteria? Can your team write the Top Model?



The success of HACKtheMACHINE: Unmanned gives the Task Force the first pieces of what they need to design, develop, and find the best capabilities in the world. It also gives the Office of Naval Research the opportunity to learn who has effective technology in order to build the invitation list for live test events in coming months.

HACKtheMACHINE Unmanned stakeholders include the Chief of Naval Research, the Navy's new Unmanned Task Force, PEO C4I, PEO IWS, and PEO USC who are all motivated to get after these hard problems fast. Join us for the Navy's premier digital experience - HACKtheMACHINE.