Search Warrant

Application for Search Warrant

DHS CyberCamp Team Ascension Christian have reason to believe that Kentucky Institute of Technology APL KIT APL, in Kentucky has information that may lead to the apprehension of people involved in the Praetorian Drones being activated.

In this assignment of establishing a plausible target for the illegal access of the Q-10 Praetorian Drone, evidence that was provided supported the theory that the Kentucky Institute of Technology Advanced Prototype Lab or the KIT APL was behind the drone entry. The information that will be uncovered through the search warrant will further back our claims.

Believing that the, uncovered through the search warrant, will provide substantial evidence to linking the Kentucky Institute of Technology to possible contacts as well as message date logs and possible IP locations linked to the recipients. Prior to the issuing of this search warrant, we had reason to believe that KIT APL was involved, through email, with a possible connection responsible for the theft of the Q-10 drones and the terrorist attack on the Turkish President, Tayvip Erdogan. The emails are believed to have further information that will supply us with the necessary evidence to finding the responsible group or culprit, whom KIT was communicating with. We believe that KIT is connected to the main perpetrator because they had programmed and installed the AI system into the Q-10 drones, which would allow them to take control of the drones and establish a weapon’s cache to carry out the intended attacks or provide another unit with the same capabilities.

KIT APL has received some funding from the Turkish military. The current state of affairs in Turkey suggests that Turkish military may be interested in removing the president. The Turkish military has a history of coups when they believe it is necessary to preserve a secular and independent turkey.

This is further supported by the source of the attack command and Lock out command. The drone recovered in Turkey had been controlled from within the Turkish nato forces. The target and lockout commands where sent from an IP address belonging to the Turkish military. The Turkish military would information on how to bypass the security. This information would be readily available from many of the kit employees and very possibly from Khalib Mehmet who formerly worked at KIT. He now works at Kadir university in Turkey.

The records sought are all emails to and from KIT APL.