

New Pentagon weapons systems easily hacked: report

9 October 2018



US Air Force F-22 Raptor: a government report says the Pentagon's weapons systems currently under development are highly vulnerable to hackers

New US weapons systems being developed by the US Department of Defense can be easily be hacked by adversaries, a new government report said on Tuesday.

The Government Accountability Office said the Pentagon was unaware of how easy it could be for an adversary to gain access to the computer brains and software of the weapons systems and operate inside them undetected.

The weak points began with poor password management and unencrypted communications, it said.

But it said access points for the systems continued to grow in number and are not always well-understood by the operators themselves, leaving even non-networked systems deeply vulnerable.

More critically, the [report](#) faulted the US military for not incorporating [cybersecurity](#) into the design and acquisition process for the computer-dependent weapons, and said weapons developers often did

not themselves adequately understand cybersecurity issues.

"Due to this lack of focus on weapon systems cybersecurity, DOD likely has an entire generation of systems that were designed and built without adequately considering cybersecurity," the GAO said.

"In one case, it took a two-person test team just one hour to gain initial access to a [weapon system](#) and one day to gain full control of the system they were testing," it said.

In another case, it said, the test team gained control of the terminals of the system's operators.

"They could see, in real-time, what the operators were seeing on their screens and could manipulate the system."

The public, unclassified version of the report did not identify which arms systems it had tested and found faults with, citing the need for secrecy.

But it said that between 2012 and 2017, the Defense Department's own testers "routinely" found dangerous cyber vulnerabilities in "nearly all" [weapons systems](#) under development.

"Using relatively simple tools and techniques, testers were able to take control of these systems and largely operate undetected. In some cases, system operators were unable to effectively respond to the hacks," it said.

The risk rises as Pentagon weapons and other systems are increasingly interconnected and their dependence on software and networking continues to rise.

The report came as the US [government](#) wrestles with what it sees as concerted efforts by government-backed hackers in Russia and China

to permeate government and private sector
computer networks to steal data or simply wreak
havoc.

© 2018 AFP

APA citation: New Pentagon weapons systems easily hacked: report (2018, October 9) retrieved 20 May 2019 from <https://phys.org/news/2018-10-pentagon-weapons-easily-hacked.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.