

DoD ([//www.fifthdomain.com/dod/](https://www.fifthdomain.com/dod/))

## What's in the \$9.6B cyber budget request?

The White House's fiscal 2020 budget request to Congress, published March 11, asked for a cyber budget of \$9.6 billion (<https://www.fifthdomain.com/dod/2019/03/11/white-house-ops-dod-cyber-budget-request/>).

The request will fund a wide variety of things under the “cyber” moniker, to include cybersecurity as well as operations.

“In terms of the broad brush of the budget, it really starts with cybersecurity. That's both hardware and software. We have to reduce the risk to [Department of Defense] information systems,” Kenneth Rapuano, assistant secretary of defense for Homeland Defense and Global Security and principal cyber adviser, said during a March 13 House Armed Services Subcommittee hearing.

According to budget materials released March 12, the \$9.6 billion breaks down with \$5.4 billion toward reducing the risk to DoD networks by investing in more cybersecurity capabilities and \$61.9 million going toward modernizing DoD's multi-cloud environment.

Rapuano said the funds also go toward research and development as to ensure the United States “out innovates” adversaries.

The request also goes toward cyber operations to include tools, training and “all of the elements necessary for us to conduct cyber operations effectively,” Rapuano added.



(<https://www.fifthdomain.com/dod/cybercom/2019/02/19/cyber-commands-2019-plan-for-new-tools/>)

**Cyber Command's 2019 plan for new tools**

(<https://www.fifthdomain.com/dod/cybercom/2019/02/19/cyber-commands-2019-plan-for-new-tools/>)

Cyber Command is moving out on several fronts to begin developing its own infrastructure and tools for cyber warriors.

**By: Mark Pomerleau**

DoD budget materials note \$3.7 billion going toward supporting offensive cyber operations and \$2.6 billion for increased training for cyber operations. \$2 billion is also going toward continued support for the cyber mission force — the 133 offensive, defensive and support teams that U.S. Cyber Command uses to conduct operations.



Moreover, \$532 million of the \$9.6 billion request, roughly six percent, is going to the headquarters of Cyber Command, Gen. Paul Nakasone, the command's head, told the committee.

Also, \$1.9 billion will go for building of infrastructure, 87 percent of which will be spread across the four locations the command has teams. The rest of that, around \$200 million, will stay within Cyber Command.

DoD budget documents also outline new funding lines for tools and capabilities Cyber Command, along with the service cyber components will utilize.



(<https://www.fifthdomain.com/dod/2018/02/20/what-the-budget-request-explains-about-cyber-commands-goals/>)

### **What the budget request explains about Cyber Command's goals**

(<https://www.fifthdomain.com/dod/2018/02/20/what-the-budget-request-explains-about-cyber-commands-goals/>)

Here are four programs and capabilities Cyber Command is looking to purchase in fiscal 2019.

**By: Mark Pomerleau**

This includes two separate funding lines for the same program element of Unified Platform, Cyber Command's major weapons system currently in development (<https://www.fifthdomain.com/dod/2019/01/10/dod-ramps-up-development-of-a-cyber-factory/>).

In a DoD budget document titled "Research, Development, Test and Evaluation Programs," Unified Platform, which is being funded by the Air Force on behalf of Cyber Command and the other services, will get \$10 million in FY20. Under another line item, but still the same program element, the document lists another \$84.7 million for Unified Platform.

The document also lists \$11.6 million for Joint Cyber Command and Control, also being funded by the Air Force on behalf of Cyber Command, for FY20. Joint Cyber Command and Control will provide combatant commanders, with enhanced situational awareness and battle management for cyberspace operations missions and forces.

On the training side, in a DoD budget document titled "Procurement Programs," the Army lists \$3 million for the Persistent Training Environment (PCTE) (<https://www.fifthdomain.com/dod/2018/10/25/cyber-operators-get-first-crack-at-training-platform/>). Funded by the Army on behalf of Cyber Command, PCTE is a much-needed capability that will provide individual and collective training, as well as mission rehearsal for cyber warriors. Such a capability currently does not exist.

It is possible when the individual services release their justification books at a later date, the funding numbers on these items will be clearer.

DoD R&D budget documents also shed light on addition cyber items the services are pursuing:

Army:

- \$52.1 million on cyberspace operations force sand force support
- \$62.2 million on defensive cyber tool development

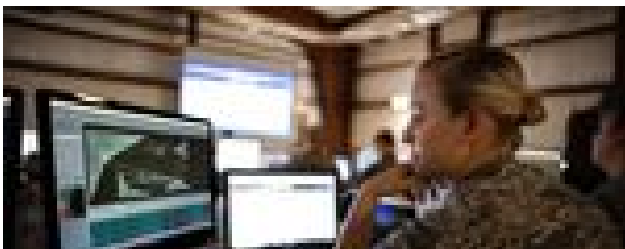
#### Navy:

- \$26.4 million on cyber operations technology development

#### Air Force:

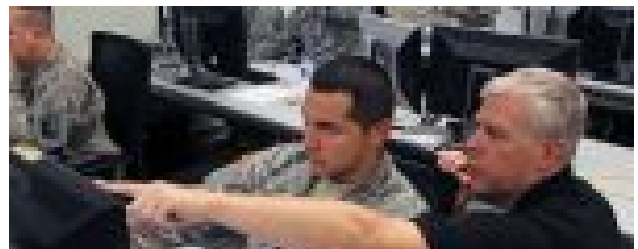
- \$198 million on cyber operations technology development
- \$16.6 million on enabled cyber activities
- \$35.1 million on distributed cyber warfare operations
- \$16.6 million on Air Force defensive cyberspace operations
- \$4.3 million on rapid cyber acquisition (<https://www.fifthdomain.com/dod/air-force/2017/11/08/how-the-air-force-is-doing-rapid-cyber-acquisition-for-offense-defense/>)

### Recommended for you



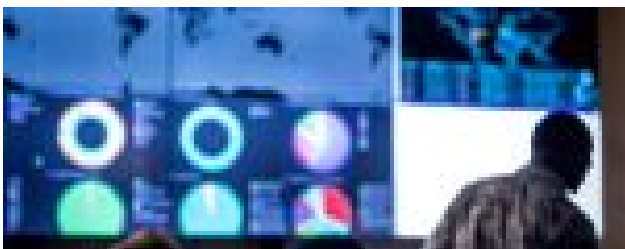
#### Here's how DoD will invest in the cyber mission

([http://www.fifthdomain.com/dod/2019/03/20/heres-how-dod-will-invest-in-the-cyber-mission/?utm\\_source=clavis](http://www.fifthdomain.com/dod/2019/03/20/heres-how-dod-will-invest-in-the-cyber-mission/?utm_source=clavis))



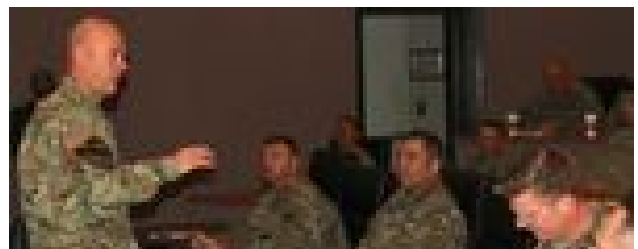
#### Where CYBERCOM wants to expand the mission force

([http://www.fifthdomain.com/dod/cybercom/2019/03/21/cybercom-wants-to-expand-the-mission-force/?utm\\_source=clavis](http://www.fifthdomain.com/dod/cybercom/2019/03/21/cybercom-wants-to-expand-the-mission-force/?utm_source=clavis))



#### The Air Force wants to start a new \$35M offensive cyber program

([http://www.fifthdomain.com/dod/air-force/2019/03/20/the-air-force-wants-to-start-a-new-35m-offensive-cyber-program/?utm\\_source=clavis](http://www.fifthdomain.com/dod/air-force/2019/03/20/the-air-force-wants-to-start-a-new-35m-offensive-cyber-program/?utm_source=clavis))



#### Cyber Command to get new chief of staff

([http://www.fifthdomain.com/dod/2019/03/22/cyber-command-to-get-new-chief-of-staff/?utm\\_source=clavis](http://www.fifthdomain.com/dod/2019/03/22/cyber-command-to-get-new-chief-of-staff/?utm_source=clavis))

### Around the Web

### Comments

## Most Watched Videos



### **How the shutdown is affecting federal cybersecurity (/video/2019/01/14/how-the-shutdown-is-affecting-federal-cybersecurity/)**

Fifth Domain speaks with Darien Kindlund, of Insight Engines on the 21st day of the federal government shutdown. (Daniel Woolfolk/Staff)  
(/video/2019/01/14/how-the-shutdown-is-affecting-federal-cybersecurity/)



#### **How to stay anonymous for feds (Part 2)**

▶ Play Video

---

(/video/2018/11/16/how-to-stay-anonymous-for-feds-part-2/)



#### **Estonia wants to shape world cyber laws on UN Security Council**

▶ Play Video

---

(/video/2018/11/12/estonia-wants-to-shape-world-cyber-laws-on-un-security-council/)



#### **A key factor to Estonia's cyber success (which the US has yet to replicate)**

▶ Play Video

---

(/video/2018/11/05/a-key-factor-to-estonias-cyber-success-which-the-us-has-yet-to-replicate/)

Top Headlines (/www..com/)

 [Newsletters \(https://link.fifthdomain.com/join/5ft/sign-up\)](https://link.fifthdomain.com/join/5ft/sign-up)  [Contact Us \(/contact-us\)](/contact-us)

---

<https://www.fifthdomain.com> © 2019 Sightline Media Group  
Not A U.S. Government Publication

**[Civilian \(/civilian\)](/civilian) [DoD \(/dod\)](/dod) [Congress \(/congress\)](/congress)  
[Critical Infrastructure \(/critical-infrastructure\)](/critical-infrastructure) [International \(/international\)](/international)  
[Workforce \(/workforce\)](/workforce) [Industry \(/industry\)](/industry) [Thought Leadership \(/thought-leadership\)](/thought-leadership)**

---

**Terms of Use**

[Terms of Service \(http://sightlinemediagroup.com/terms-of-service/\)](http://sightlinemediagroup.com/terms-of-service/)

[Privacy Policy \(/privacy\)](/privacy)

()

()

**Get Us**

[Newsletters & Alerts \(https://link.fifthdomain.com/join/5ft/sign-up\)](https://link.fifthdomain.com/join/5ft/sign-up)

[RSS Feed \(/rss\)](/rss)

()

()

**Contact Us**

[Help & Contact Info \(/contact-us\)](/contact-us)

[Advertise \(/advertising\)](/advertising)

()

()

**About Us**

[About Us \(/about-us\)](/about-us)

[Careers \(https://boards.greenhouse.io/sightlinemediagroup?gh\\_src=cpxe2a1\)](https://boards.greenhouse.io/sightlinemediagroup?gh_src=cpxe2a1)

()

()

---

[Military News \(https://www.militarytimes.com\)](https://www.militarytimes.com) [Air Force News \(https://www.airforcetimes.com\)](https://www.airforcetimes.com)

[Army News \(https://www.armytimes.com\)](https://www.armytimes.com) [Marine Corps News \(https://www.marinecorpstimes.com\)](https://www.marinecorpstimes.com)

[Navy News \(https://www.navytimes.com\)](https://www.navytimes.com) [Defense News \(http://www.defensenews.com\)](http://www.defensenews.com)

[Federal News \(http://www.federaltimes.com\)](http://www.federaltimes.com) [C4ISR \(http://www.c4isrnet.com\)](http://www.c4isrnet.com)

[Cyber \(http://www.fifthdomain.com/\)](http://www.fifthdomain.com/) [History \(http://www.historynet.com/\)](http://www.historynet.com/)

---