DoD

(/dod/)

CENTCOM chief: The future of warfare demands more cyber authorities

By: Justin Lynch (/author/justin-lynch) 3 days ago

The Pentagon has received more power to conduct cyber operations in the past 18 months. But for the top Army commander in the Middle East and Central Asia, the new authority is not enough.

The head of U.S. Central Command, Gen. Joseph Votel, wrote in a Dec. 18 paper that the Pentagon must "normalize" electronic warfare and cyberattacks and incorporate them into daily operations.

"Normalizing the cyberspace domain means broader authorities that are more responsive than current bureaucratic processes," Votel wrote (https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Fall%202018/CDR_V3N3_VOTEL_JULAZADEH_LIN_OperationalizingInfoEnvironment_ARTICLE_E2.pdf?ver=2018-12-18-102425-550) in the Army's Cyber Defense Review. "It also means we need simple and streamlined organizations and processes to increase lethality and enhance performance."

The paper was coauthored by Votel, Maj. Gen. Julazadeh and Maj. Weilun Lin.

"Our failure to operationalize and normalize the cyberspace domain effectively cedes it to our adversaries, gives them a competitive advantage and, ultimately, creates an increased attack vector against our objectives," the authors said.

President Trump gave the Pentagon new authorities to conduct cyber operations in August and minimized the process where other agencies can object to cyberattacks, known as "deconfliction."

Secretary of Defense Jim Mattis can conduct hacking operations without approval (https://www.fifthdomain.com/congress/2018/12/10/behind-the-white-houses-plan-to-be-more-aggressive-in-cyberspace/) from the White House so long as they do not interfere with the American "national interest," according to four current and former White House and intelligence officials who were either part of internal deliberations or briefed on the changes.

Yet some current and former U.S. officials are skeptical that the new authorities will mean more effective hacking operations for the Pentagon, because it does not solve the nuances of cyberattacks.

But the new mandates do not go far enough for the three officer authors, who argued that cyberwarfare should be under the same authorities as other types of operations.

"We must not see cyberspace as drastically different and separate from other domains that we create new processes to prepare, plan and fight in this new domain. We continue to seek processes that smooth and simplify operations, reducing friendly friction and accelerating decision-making."

Current and former Pentagon officials have pointed to conducting cyberattacks against enemies that use networks of neutral or partner nations as an area where the Pentagon has changed its decision-making process in recent years. Those officials also pointed to how the Pentagon was able to use hybrid warfare tactics during the 2016 liberation of Mosul, Iraq, as a textbook example of future hybrid operations.

Votel, Julazadeh and Lin echoed the sentiment of other Pentagon officials who have advocated for cyberattacks, electronic warfare and other information operations to be integrated earlier in military operations.

“We need to proactively execute cyberspace and information operations early in 'Phase 0 / steady state’ of the planning process — well before operation execution. Only then can we shape the [information environment], hold our adversaries’ capabilities at risk and execute at the speed of war,” the three wrote.

For example, Pentagon officials say they closely monitored Russia’s 2014 hybrid war in Ukraine and learned from Moscow’s tactics. (https://www.fifthdomain.com/smr/ausa-cyber/2018/10/09/how-russian-hybrid-warfare-changed-the-pentagons-perspective/)

Votel, Julazadeh and Lin shed light on the changes, writing that information operations were previously “integrated as an afterthought.” Yet over the last two years, Central Command has incorporated cyberattacks, electronic warfare and military deception at the “strategic level.”

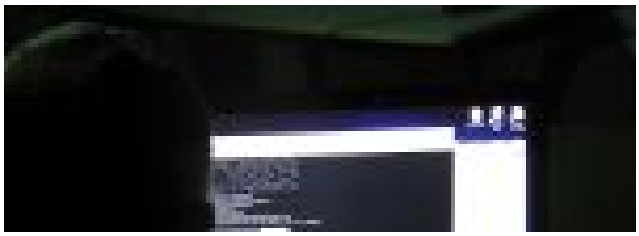
And this hybrid warfare has driven new acquisition demands in the Pentagon.

“We need technology and capabilities to keep pace with the operational environment and continue to build the partnerships to do so,” the three officers wrote.

In recent years, Central Command has bolstered its hybrid warfare through new contracts. The centerpiece (https://www.businesswire.com/news/home/20170719005430/en/SAIC-Awarded-621-Million-U.S.-Central-Command) of that effort is a July 2017 contract worth $621 million to Science Applications International Corporation for IT support to Central Command that could last seven years.

In August 2018, Vistra communications was also awarded (http://www.fbodaily.com/archive/2018/08-August/26-Aug-2018/FBO-05054667.htm) a $22 million contract to support offensive and defensive cyber operations for Central Command.

Recommended for you



US spies warn of increase in supply chain vulnerabilities

(http://www.fifthdomain.com/industry/2018/08/23/us-spies-warn-of-increase-in-supply-chain-vulnerabilities/)

A new target for hackers? Satellites

(http://www.fifthdomain.com/dod/2018/04/11/a-new-target-for-hackers-satellites/)

Emerging ‘hyperwar’ signals ‘AI-fueled, machine-waged’ future of conflict

(http://www.fifthdomain.com/dod/2017/08/07/emergin hyperwar-signals-ai-fueled-machine-waged-future-of-conflict/)

Here's how the Army wants to integrate cyber, EW into operational formations

(http://www.fifthdomain.com/dod/army/2017/10/02/heres-how-the-army-wants-to-integrate-cyber-ew-into-operational-formations/)

Around the Web

Comments

Most Watched Videos

▶ Play

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

Lance Cottrell, chief scientist at Ntrepid, shows government workers how to remain anonymous online. (Daniel Woolfolk/Staff)
(/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/)

Five Bits from Cybercon 2018

▶ Play Video

(/video/2018/11/02/five-bits-from-cybercon-2018/)

Top Headlines

Newsletters (http://link.fifthdomain.com/join/5ft/sign-up) Contact Us (/contact-us)

(https://www.linkedin.com/company/fifth-
(https://twitter.com/theFifthDomain2 https://www.fifthdomain.com © 2018 Sightline Media Group
(https://www.facebook.com/FifthDomain/) Not A U.S. Government Publication

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

Terms of Use
Terms of Service (http://sightlinemediagroup.com/terms-of-service/)
Privacy Policy (/privacy)
()
()

Get Us
Newsletters & Alerts (http://link.fifthdomain.com/join/5ft/sign-up)
RSS Feed (/rss)
()
()

Contact Us
Help & Contact Info (/contact-us)
Advertise (/advertising)
()
()

About Us
About Us (/about-us)
Careers (https://boards.greenhouse.io/sightlinemediagroup?gh_src=cpxe2a1)
()
()