All Those Pentagon IP Addresses

All Those Pentagon IP Addresses

by **Joseph P. Farrell**, *Giza Death Star*
May 5, 2021

Today's blog is about a story so unusual that I have absolutely no idea what to make of it. That's not to say I don't have plenty of high octane speculations about it, but even then, I'm left with even more uncertainty about my usual uncertainty about my high octane speculations. In fact, I'm so uncertain I don't even know if the prior sentence even made sense, hence I'm filing this one under "you tell me." That said, the reason I'm blogging about it is because of all the stories and articles I received this past week, this one nearly tied with the story about those strange directed energy-mind manipulation attacks going on in Swampington, D.C., and like that story, this one too originates – in all its fetid curiosity – from the same place. So again, thanks to all of you who shared this story.

And it's a strange one, so I'm going to present three of the versions of it that people sent along, to underscore how strange it is:

The big Pentagon internet mystery now partially solved

The big Pentagon internet mystery now partially solved Daily Mail

Why The Pentagon Handed Control Of Its 175 Million IP Addresses To One Tiny Firm

You'll note the first two articles are the AP version of the story by Frank Bajak. And the story is relatively simple in and of itself: the Pentagon – or Pentagram as we like to call it – has handed over control of a *bunch* of its internet IP addresses to a *very* small firm about which virtually nothing is known. Citing the Mr. Bajak's article:

> *A very strange thing happened on the internet the day President Joe Biden was sworn in. A shadowy company residing at a shared workspace above a Florida bank announced to the world's computer networks that it was now managing a colossal, previously idle chunk of the internet owned by the U.S. Department of Defense.*
>
> *That real estate has since more than quadrupled to 175 million addresses – about 1/25th the size of the current internet.*
>
> *"It is massive. That is the biggest thing in the history of the internet," said Doug Madory, director of internet analysis at Kentik, a network operating company. It's also more than twice the size of the internet space actually used by the Pentagon.*
>
> *After weeks of wonder by the networking community, the Pentagon has now provided a very terse explanation for what it's doing. But it has not answered many basic questions, beginning with why it chose to entrust management of the address space to a company that seems not to have existed until September.*
>
> *The military hopes to "assess, evaluate and prevent unauthorized use of DoD IP address space," said a statement issued Friday by Brett Goldstein, chief of the Pentagon's Defense Digital Service, which is running the project. It also hopes to "identify potential vulnerabilities" as part of efforts to defend against cyber-intrusions by global adversaries, who are consistently*

> *infiltrating U.S. networks, sometimes operating from unused internet address blocks.*
>
> …
>
> *Madory said advertising the address space will make it easier to chase off squatters and allow the U.S. military to "collect a massive amount of background internet traffic for threat intelligence."*
>
> *Some cybersecurity experts have speculated that the Pentagon may be using the newly advertised space to create "honeypots," machines set up with vulnerabilities to draw hackers. Or it could be looking to set up dedicated infrastructure – software and servers – to scour traffic for suspect activity.*

OK, that seems clear enough…

… until one probes the massive size of what's involved. Basically, 175,000,000 internet addresses is almost one address for every two people in the whole USA, give or take a few decimals… that's a *lot* of internet space just to be running threat assessments. In fact, it's more space than all of AT&T or China. And as the AP article points out, why hand it over to a small company that shares addresses in a post office in a UPS store and that does not return calls.

Which brings us to the third article linked above, and to this little tidbit:

> *Brett Goldstein, d**irector of the Defense Digital Service (DDS)**, said the Pentagon had authorized the pilot program to "assess, evaluate, and prevent unauthorized use of DoD [Department of Defense] IP address space," adding that it could help "identify potential vulnerabilities." (Boldface emphasis added)*

So what is the "Defense Digital Service" or DDS? Well, L.G.L.R. spotted *this* article and sent it along:

[Defense Digital Service Delivers Mission-Aligned Tech for DOD]

You'll note that the article is from the US Department of Defense itself, and accordingly, much of the article is standard boilerplate: long on fluffy self-promotion, and short on juicy details. But there are some intriguing tells nonetheless. Consider the following:

> *DDS has roughly 70 technologists, including 19 active-duty service personnel. The civilians tend to come from private-sector backgrounds and are on two-year term-limited appointments. Goldstein refers to his team, which includes engineers, designers and developers, as a "SWAT team of nerds" that reports to the secretary of defense.*
>
> …
>
> *DDS experts don't dwell in the office, either. They travel to where service members are to see how DDS can help use technology to address challenges. Goldstein said he's been to Afghanistan three times so far, and that the project pipeline for DDS originates directly through the critical needs of the services and combatant commands.*
>
> *He also said he's recently been visiting various commands as well, including U.S. Transportation Command, Army Cyber Command, U.S. Central Command, U.S. Special Operations Command, and U.S. Strategic Command as he works to further hone DDS priorities to have the biggest impact possible.*
>
> …
>
> *Another project focused on strengthening the security of DOD systems. In the private sector, many of the largest companies use "bug bounty programs" or have their systems evaluated by vetted outsiders known as "ethical hackers" to find and*

> *report bugs — and then pay cash when flaws are discovered. The federal government had never done that before until DDS launched the "Hack the Pentagon" program in 2016. It was the first federal bug bounty program, and it has led to thousands of vulnerabilities reported in government systems.*
>
> …
>
> *Looking forward, some near-term efforts under Goldstein will include expanding the DDS "Jyn" program that pairs cyber soldiers and other military tech talent with DOD experts on special projects; launching a pilot to help modernize and automate portions of the security clearance process; building out a new satellite office in Augusta, Georgia, near the Fort Gordon community; and continuing to advise on the JEDI cloud procurement.*

While I certainly do not discount the possibility that there is disinformation here, and even the possibility that the whole "Defense Digital Service" might just be a front for a much deeper more sophisticated but unknown department, just as I do not discount the strange little Florida start-up company might be the same, for the sake of argument, let us take the above statements at face value. Doing so, what do we have? We have

(1) " a swat team of nerds" that

(2) travels around the world "networking" with various command and control structures of the Defense Department, notably including "Army Cyber Command" and "US Special Operations Command";

(3) it's involved in increasing cyber security, presumably via "bug bounty programs," and

(4) "pairs cyber soldiers and other military tech talent with DOD experts on 'special projects'".

In other words, we're looking at a full scale cyber counter-intelligence, intelligence, and hacking operation. Of interest here is that "bug bounty program," which would certainly fit the bill for cyber-counter-intelligence operations, for such operations are bound to be targets for infiltration by foreign intelligence services wanting to cloak their very real cyber-operations within the program.

But there's a couple of areas curiously *absent* from the boilerplate: (1) *space*, and (2) *financial flows*. The latter would, indeed, be a rich data stream both for cyber-intelligence and cyber-counter-intelligence operations, and I cannot help but think that this may be part of what's covered under the generic "special projects". And the importance of space to cyber-operations and the military goes without saying.

I cannot help but think that this is also somehow linked to the Bidenenko regime's warning to Russia that it intended to "send a message" whose true significance would be appreciated only by Russia, and not the general public. I wonder, in other words, if we're not looking at that message in some form or fashion.

If so, then one might remember that any electrical circuit can be used as a conduit for mind manipulation technologies: cyber-warfare meets mind-manipulation tech as it were. If so, then we might also be looking at a new phase of assymetrical warfare operations.

On and on I could go, but as I said, this is such a strange story that it's a case of "you tell me".

See you on the flip side…

Connect with Joseph P. Farrell