OPERATION BUCKSHOT YANKEE AND WIKILEAKS

Ellen Nakashima had a long article on Thursday using the 2008 thumb drive infection of DOD's networks (including, she mentions in passing, the top-secret JWICS system) to describe the evolution of our approach to cybersecurity.

The whole thing is worth a close reading. But I'm particularly interested (as always) in reading it with WikiLeaks in mind. As Nakashima notes after describing the supposedly stringent response to the 2008 infection, which included "banning" thumb drives, Bradley Manning is suspected of downloading entire databases via the same means, removable media.

> As the NSA worked to neutralize Agent.btz on its government computers, Strategic Command, which oversees deterrence strategy for nuclear weapons, space and cyberspace, raised the military's information security threat level. A few weeks later, in November, an order went out banning the use of thumb drives across the Defense Department worldwide. It was the most controversial order of the operation.
>
> Agent.btz had spread widely among military computers around the world, especially in Iraq and Afghanistan, creating the potential for major losses of intelligence. Yet the ban generated backlash among officers in the field, many of whom relied on the drives to download combat imagery or share after-action reports.
>
> [snip]
>
> The ban on thumb drives has been partially lifted because other security measures have been put in place.
>
> [snip]

> What is clear is that Agent.btz revealed weaknesses in crucial U.S. government computer networks — vulnerabilities based on the weakest link in the security chain: human beings. The development of new defenses did not prevent the transfer of massive amounts of information from one classified network to the anti-secrecy group WikiLeaks, an act that the government charges was carried out by an Army intelligence analyst.

Now, first of all, is it really a stunning revelation that introducing removable media into a secret or top-secret network might be a "vulnerability"? It took an attack to make that clear?

And if DOD has put so many security measures in place, then how did the Creech Air Force Base, which controls our drones, get infected?

Then there's Nakashima's discussion of how DOD could respond to "an attack" in the United States. She makes it clear that in the aftermath of the thumb drive attack, the military decided (to its chagrin) its rules of operations should not allow it to bring down a server in this country.

> By the summer of 2009, Pentagon officials had begun work on a set of rules of engagement, part of a broader cyberdefense effort called Operation Gladiator Phoenix. They drafted an "execute order" under which the Strategic and Cyber commands could direct the operations and defense of military networks anywhere in the world. Initially, the directive applied to critical privately owned computer systems in the United States.
>
> Several conditions had to be met, according to a military official familiar with the draft order. The

> provocation had to be hostile and directed at the United States, its critical infrastructure or citizens. It had to present the imminent likelihood of death, serious injury or damage that threatened national or economic security. The response had to be coordinated with affected government agencies and combatant commanders. And it had to be limited to actions necessary to stop the attack, while minimizing impacts on non-military computers.
>
> [snip]
>
> The debate bogged down over how far the military could go to parry attacks, which can be routed from server to server, sometimes in multiple countries. "Could you go only to the first [server] you trace back to? Could you go all the way to the first point at which the attack emanated from? Those were the questions that were still being negotiated," said a former U.S. official.
>
> The questions were even more vexing when it came to potentially combating an attack launched from servers within the United States. The military has no authority to act in cyberspace when the networks are domestic — unless the operation is on its own systems.

Ultimately, Nakashima seems to say, the government decided DOD should not be able to disable a server in the US.

But then, the next year, someone disrupted WikiLeaks servers, including—probably using political, not cyber force—its US-based Amazon servers. Aside from the supposedly "former" special forces member who claimed credit for the first attacks, we've never had adequate explanation of how and under what authority the

government brought down WikiLeaks.

And check out the standards—more of the Executive Branch deciding who our enemy is in secret—they used.

> The provocation had to be hostile and directed at the United States, its critical infrastructure or citizens. It had to present the imminent likelihood of death, serious injury or damage that threatened national or economic security.

Did someone decide WikiLeaks met these terms? If so, is the standard for a threat to national security so low that the WikiLeaks disclosures would merit such an action? Really?

And where does the use of other authorities—pressuring Visa and MasterCard and PayPal and Amazon to stop doing business with an entity—come into this?

Nakashima's sources seem to want to suggest that they have no authority to stop attacks in the US. But someone does—and has already used it. And used it against an entity DOJ had not yet created an exception for in its definition of media.