COMPARE DOD'S AUTONOMY TO ENGAGE IN CYBER-WAR WITH OBAMA'S CLOSE CONTROL OVER DOD DRONE TARGETING

It will likely be some time, if ever, before one of our enemies succeeds at doing more than launching limited, opportunistic drone strikes at the US. By contrast, every day brings new revelations of how our enemies and rivals are finding new vulnerabilities in American cyber-defense.

Which is why it is so curious to compare this account of the multi-year process that has led to an expansion of DOD's authority to approve defensive cyber-attacks with this account of Obama's close hold on DOD's drone targeting.

In both cases, you had several agencies — at least DOD and CIA — in line to execute attacks, along with equities from other agencies like State.

> An interagency process had been started because cyber concerns confront a variety of agencies, the intelligence community and DoD as well as State, Homeland Security and other departments, with each expressing views on how the domain would be treated.

For much of Obama's term, it seems, both DOD drone attacks outside of the hot battlefield and cyberattacks had to be approved by the White House. With drones, Obama wanted to retain that control (over DOD, but not CIA) to prevent us from getting into new wars.

> But from the outset of his presidency, Obama personally insisted that he make

> the final decision on the military's kill or capture orders, so-called direct action operations. Obama wanted to assume the moral responsibility for what were in effect premeditated government executions. But sources familiar with Obama's thinking say he also wanted to personally exercise supervision over lethal strikes away from conventional battlefields to avoid getting embroiled in new wars. As responsibility for targeted strikes in places like Yemen, Somalia, and, over time, Pakistan shifts to the military's Joint Special Operations Command, Obama will be the final decider for the entire program.

With cyber, White House control was designed partly to limit blowback — almost the same purpose as his micromanagement of drone targeting — but also to mediate disputes between agencies.

> In every instance where cyber was involved, the NSC had to be involved. That helped settle some of the disputes between agencies by limiting any independent application of cyber capabilities, but was useful neither for expediting any cyber action nor for integrating cyber into larger military capabilities. Several sources said that this has slowed the integration of cyber into broader military tactics, possibly giving rivals without the same hesitation, like China, a chance to become more adept at military cyber.
>
> [snip]
>
> Because every decision had to be run through the West Wing, potential political blowback limited the use of cyber tools, the former senior intelligence official said. "If they can't be used without a discussion in the West Wing, the president's got no

> place to run if something goes wrong when he uses them," he said. Those decisions included what to do if the US confronted a cyberattack.

But over the course of the Obama Administration, DOD lobbied to increase its autonomy in both areas, in drones via the year-long process of crafting a drone rulebook, and with cyber, via the three year process of drafting new standing rules of engagement.

It had far more success in its efforts to expand autonomy with cyber.

With drone warfare, CIA pushed to let DOD have the same authorities to launch strikes without Presidential oversight that it had.

> Sources familiar with the process say no issue was more contentious than the question of what role the president should have in final killing decisions. The uniformed military, including the joint chiefs of staff, pushed to take the president out of the process. Once the president approved a particular battle plan in a country, individual targeting decisions should be left up to the regional commanders, they argued. Officials at the CIA, who had fought successfully to maintain control over its own targeting in the early days of the administration, backed the military.

But ultimately, Obama refused to expand DOD's autonomy to exercise the same autonomy that CIA already enjoys.

> A draft version of the new institutionalization policy, known informally as "the playbook," even contained the proposed change, the sources say. But after an intense counteroffensive by officials at the State Department and Justice Department, the status quo was restored. According

> to one official who participated in the discussions, it came down to a question of what level of accountability was required when the government was making grave killing decisions far from the traditional battlefield: “It didn’t make sense that while we were on the one hand raising the bar for these decisions, we would also remove the president from the decision-making chain.”

Contrast that with cyberwar, where in each of several reviews, DOD (specifically, General Keith Alexander, head of both NSA and CyberCommand) won greater autonomy, at least for defensive cyber responses.

> Not long afterward, that draft was rejected by a deputy of Gen. Keith Alexander, head of CYBERCOM and director of the National Security Agency, because it fell short of where “the SecDef wanted it to go,” said a former defense official.
>
> The problem was that the document didn’t allow for a sufficiently assertive response, the official added. In its efforts to achieve balance, the draft didn’t accommodate the strong stance the administration, and specifically CYBERCOM, wanted to take.
>
> So the rules were drafted again, designed to be “forward leaning,” permitting a stronger response. Once again they were rejected.
>
> [snip]
>
> According to the former defense official with knowledge of earlier drafts, the version on the verge of completion is “way far” from previous versions, authorizing far more assertive action than had been previously considered.

Perhaps this comparison is too strained. As described, at least, DOD will only have autonomy to engage in responses to cyber-attacks. With preemptive offensive attacks, the White House will remain in the loop.

To some level, the expected continuation of signature strikes in Pakistan, which inaccurately or not have been excused as a response to attacks on US troops stationed in Afghanistan, is similar to DOD's permission to engage in defensive counterattacks.

But the comparison is useful, I think. because it raises questions about where we should have in the past and should going forward be exercising closer oversight. I'm all in favor of sharply limiting the number of times we assassinate a human off the battlefield. But I also believe that cyber-war — even attacks billed as a counter response to an attack — have led to and will likely to lead to far more blowback even than drones.

With StuxNet we seem to have normalized a pretty aggressive bar for cyber-attacks. Each new example of doing so will, because of our extreme vulnerability, expose us to far more dangerous blowback.