Have you ever heard of the CyberKnife? It sounds like a great weapon, doesn’t it? Something you could just stab it into the heart of every rogue fleet on the high seas. And you can tell it’s cool because it has the word “cyber” in it.

Everywhere you turn these days, it’s cyber-this and cyber-that. Never mind that this prefix is fungible at best, and takes on whatever meaning the speaker imbues it with in that moment. It seems the easiest way to show that you are hip to emerging technologies in warfare is to liberally sprinkle the word “cyber” into any document or context.

This cannot continue. Words matter, and before we can properly employ emerging technologies in armed conflict we must learn how to speak intelligently about the conduct of military operations in and from cyberspace. So what do you do? Where can you turn? How do you even begin? Here are five simple suggestions from a newly-minted MOC warfighter with a background in cyberspace operations.

One: Stop over-promising in order to avoid under-delivering.

Ever since William Gibson wrote that cyberspace is “a consensual hallucination [of] unthinkable complexity,” this discipline has been viewed through the lens of near-mysticism. Similarly, in the early days of aviation, it appeared that taking to the sky could solve any of man’s problems. Charles Lindbergh called it “drinking the wine of the gods.” And yet here we are: the Air Force did not make everything else obsolete. Therefore, whenever you are compelled to write a plan in which “cyber” gets you there from here, you need to do some research to help scope your expectations.

Two: Do your homework.

One cannot, as a general rule, speak authoritatively on behalf of surface, air, or submarine warfare without having ever conducted it, yet well-meaning officers are daily thrown into senior roles in cyberspace operations without adequate background or training. Almost everyone seems to have come late to the game. So how can you avoid looking like one more paper tiger in the cyber jungle? We have a pub for that. Please, please read JP 3-12.1 And PPD-20.2 And the DoD Cyber Strategy.3 And just about anything else you can get your hands on. In learning the right vocabulary, you will also become familiar with the art of the possible – the one that exists outside of movies.

Three: There is no such thing as a cyber target.

This is a key point, and worth repeating: there is no such thing as a cyber target. A

---

1 Joint Publication 3-12(R) Cyberspace Operations, 5 February 2013
2 Presidential Policy Directive 20 [ Classified], October 2012
3 Department of Defense Cyber Strategy, April 2015
target is just a target; “An entity or object that performs a function for the adversary considered for possible engagement or other action.” (JP 3-60)\(^4\) As in many emerging technological fields, in this arena one may often run into a capability in search of an objective. This is a bad way to spend taxpayers’ resources. Instead, begin with the objective in mind. Make a proper plan with a center-of-gravity analysis and all of the other critical thinking tools found in JP 5-0 and NWP 5-01, and proceed from there.

**Four: Talk to me, (cyber-) Goose.**

No matter what anyone says, cyberspace operations are just another tool in the toolkit. They are a *means* to create an *effect*, like any other tool. Anyone who says otherwise has probably not completed suggestions One through Three. Now that you have your plan - or better yet, while you are forming your plan - go start a brainstorming session with your N- or J-39-types, wherever your staff has hidden them away. Justify why you feel like you need to employ some sneakiness. The information warrior, in turn, should be asking you questions. While you may not be privy to everything that lies behind the green door, you are hopefully an expert on the effect you want to direct against the enemy. Working together, you can sort out whether you are trying to go after something that is best prosecuted in and from the cyberspace domain (for plausible deniability, for example), or whether you want to go after something that is important because of its role in your adversary’s command and control network, but which may be best to pursue through traditional kinetic means. No matter how sexy the sneaky option may seem, remember that it is always faster to just blow something up.

**Five: You can’t always get what you want.**

Our current cyberspace capabilities grew out of decades of work from the national intelligence community. As a general rule, these things take an excruciatingly long time to build and are very easily lost, compromised, or countered. In fact, unless you are going after an enduring adversary with an established infrastructure, all the advanced technology in the world may not be able to help you. If there are capabilities that can be brought to bear, the commander conducting a cyberspace attack must balance the benefit gained by using this weapon with the risk to future intelligence collection efforts and the potential for collateral damage to similar operations. That is to say, if “cyber” were an M16, you could only shoot it once and then every M16 in the DoD would jam forever. This means that the farther you get from just stealthily collecting information, the more likely national command authorities would deny your cyber effects request and tell you to just go light the target up the old-fashioned way. If you ask for cyberspace intelligence, surveillance, and reconnaissance (ISR) or cyberspace operational preparation of the environment (OPE), you may indeed get it because these activities are among the discipline’s core competencies and present pretty low risk to ongoing operations. Otherwise, it often just isn’t worth risking the broader interests of the country. When you look at it from this perspective, you can see that “cyber” is

\(^4\) Joint Publication 3-60 Joint Targeting, 31 Jan 2013
indeed a strategic weapon, because the consequences can be felt well above and beyond the operational level.

This is not to discourage planners and other staff officers from inviting “cyber” into their professional lives. We just need to collectively change the way we think and talk about it, so we use it for the right situations. By having realistic expectations, doing your homework, focusing on effects and not the means, and remembering that cyberspace activities can have strategic-level implications, you can get to yes with your friends behind the green door.

Oh, and that CyberKnife? It turns out it is better suited for a surgical strike – it’s a robotic cancer treatment system. Too bad. That would have been way cool.

*CDR Audrey Adams is the Capabilities Branch Chief for Commander, U.S. Fleet Cyber Command / U.S. TENTH Fleet.*