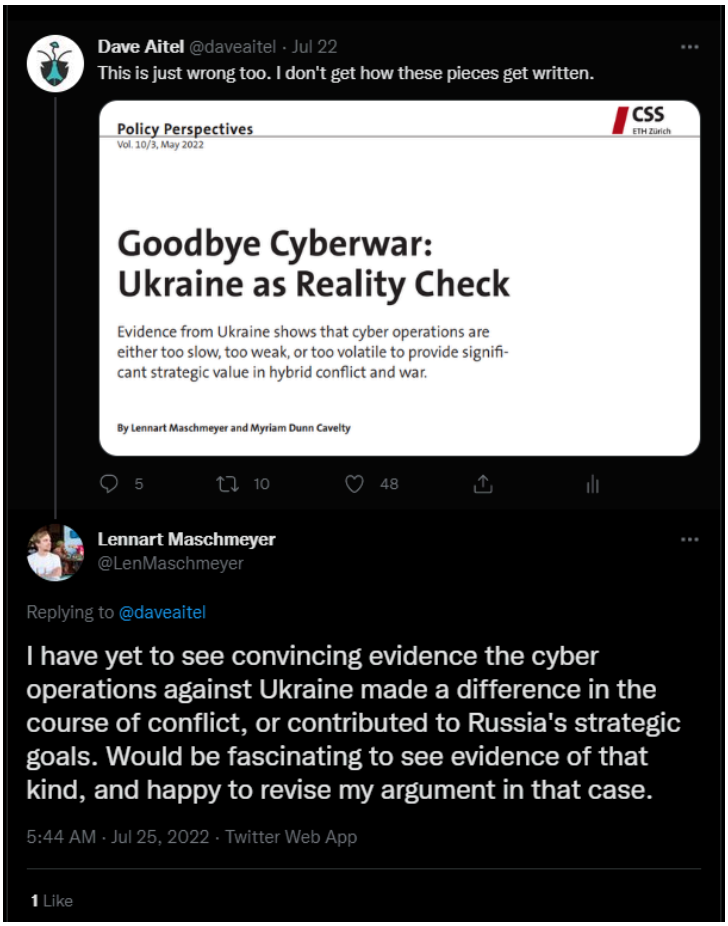

Notes from Dave Aitel (representing no govt or other organization)

Link to original piece from (L. Maschmeyer and M. Cavalty):
https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/PP10-3_2022-EN.pdf

A good title for any piece is “Goodbye cyberwar, hello integrated cyber operations” which explains better what we’ve been seeing.

The subtitle to the piece is interesting as well:
“Evidence from Ukraine shows that cyber operations are either too slow, too weak, or too volatile to provide significant strategic value in hybrid conflict and war.”

Significant strategic value is not a clearly defined term, which probably makes it pointless to argue about. But what IS clear is that we don’t have even the beginnings of an understanding for how the Ukrainian war has progressed. We don’t know how many casualties there were, on either side, we don’t know how many pieces of equipment were destroyed, broke down, or whether things simply ran out of gas and were abandoned. We don’t know ANYTHING. So saying “Cyberwar didn’t happen” is wrong because obviously the right answer is: We don’t know

the impact of literally anything and it's hard to measure "impact" even in the best of circumstances.

One interesting article, and I hate quoting news articles on this sort of thing, because you end up falling into clickbait cycles, is this one:
https://www.cyberscoop.com/russian-forces-ukrainian-isp-blackmail/

The reality here is this: extending your ICT surveillance bubble across a community is how you actually "take ground" in the 21st Century. It's not YOURS until you move it behind your national firewall. That's "contributing to strategic goals" enough for me!

But beyond that, to the value of cyber operations in general:

- Russian plans were leaked continuously by the US in the run up to the war, and this delayed the war by two weeks, which had a massive impact on the outcome.[1]
- ViaSat is a direct command and control strike against the Ukrainians. That sounds like strategic value, even if there is no current information on what the impact was (and maybe never will be?). The paper says "Meanwhile, a disruption of the Viasat satellite communications network evidently aimed at cutting Ukrainian military communications failed to produce a measurable effect on these communications. " But…we don't know that? Are we going to believe everything we hear from the Ukrainians? Also, I think they said it was impactful. HAVING A BACKUP IN PLACE DOES NOT MEAN THE EFFECT DID NOT HAPPEN. Often forcing someone to a less secure backup plan is the GOAL of OCO.
- Wipers are being found all over the place - sometimes because they've already executed, I assume? The Russians aren't writing these for fun!

It's true that Pipedream/incontroller was "found" before it was used. This sounds like the result of successful Counter Cyber Operations. There's a recent paper on what the likely or possible response from an adversary is to CCO that goes into this stuff in some depth, and it looks like we might be seeing some of that play out in real time, not just in Ukraine but also in the ongoing escalation of the cyber conflict between Israel and Iran.

From the paper: "Overall, there is no evidence that any of the Russian-sponsored operations or, in fact, any of the operations related to this conflict (including the various hacktivist "armies" that have sprung up) measurably affected the course of the conflict, provided observable tactical advantages – such as sabotaging military equipment or disrupting enemy communications during battle – or produced strategic value."

We absolutely do not know this. When OCO works well, it often is viewed as "things just going wrong". Your radar just happens to malfunction. Your trains are held at the station because the switching network is faulty today for some reason. Your comms just happen to not be able to key up properly - probably need to switch to unencrypted comms, wait, now everyone is yelling

[1] Honestly we have no idea how these plans kept getting collected. Could be HUMINT, or standard SIGINT, or OCO or just the result of good analytical tradecraft.

at us over our own radios and we can't even hear our orders! Hey our generals keep getting exploded at long range. Weird. Must be bad luck. This is why Predatory Sparrow has to release a whole video of their attack happening on a TWITTER ACCOUNT and even then people don't believe it.

The honest thing to say would have been: It's far too soon to know what happened in Ukraine, via Cyber or otherwise.

The paper leans heavily on this idea of the "Trilema" that offers a tradeoff in cyber operations between "speed, effects intensity, and control over effects". But addressing this trilemma (and the other drawbacks inherent in OCO) is, of course, the goal of any organization worth their salt in this space. You build and buy 0day so you can have rapid and covert access to what you need, and you invest in implants and toolchains which you have on the shelf so you can work on effects intensity and control over effects in a predictable way when the time comes. THAT IS WHAT PIPEDREAM IS.

This is what the literature would point to as "arsenal management". It's more complicated in a contested space of course, but that's why this game is fun, and not just pachinko but with computers.