Collider/Disrupter Event TFA#3 Q&A Telecon Transcript
07 March 2024

TFA #3. C5I / Sustainment and Protection / "Digital" Camouflage

Technology Focus Area Advocate: SOF AT&L-ST
Modernization Priority: Battlespace Awareness, Multi-Domain Communication and Computing

1. **How many companies are expected to be selected for "path forward"?**
   No set number, could be zero, could be one, could be more. Just depends on if there's relevant technology that we think would make a good fit over.

2. **Could you provide more examples to illustrate the need to reduce/conceal SOF operator's signature in the virtual/digital domain?**
   Typically, SOCOM's trying to hide the physical signature of our operator and their equipment and platforms and that's you know the typical spectrums, visible thermal radar acoustics and historically that was always on the battlefield. You know this new world we live in with ubiquitous technical surveillance where everything is a sensor, and everything collects data. It's now difficult to hide our operators and frankly their friends and families, you know that hide their digital signature and that is before, during and after even a particular conflict or a mission. So, these digital vectors you call them, facial recognition, license plate recognition, cell phones or cell networks and 5G, Wi-Fi, vehicle telematics, financial transactions, CCTV, social media, online advertising, I mean the list goes on and on. Frankly, it's a giant problem. On the government side, we have not identified any solution yet and there is not going to be one solution to solve all of those. But we're looking for anything, you know, software, hardware, new con OPS that would minimize our adversary's ability to detect and track these digital signatures. Often the complete elimination of a signature is a signature in and of itself. So we need to be able to spoof or decoy or hide within the noise for all of those vectors I mentioned.

3. **Any guidance on ROM parameters which are typical for Collider?**
   No set parameters. Honestly, we're driving off how good of an idea it is or not and if it's an operational gap or capability gap. It's a very broad area. There's a lot of unknowns and also a lot of unknowns to us. If you have a good idea that you think would figure in well to that area that we just described, then go ahead and submit its total length and total amount. Again, that's dependent upon effort. If we could have something as short as a year, maybe two to three years, the total cost again will depend on the level of effort and what you're submitting over. The TRL (Technology readiness levels) ranges from TRL 1 to 9, one being basic research, 9 being fully fielded operational, full sustainment in S&T Science and Technology Directorate. We're working with stuff as low as TRL 2 in some cases, but generally TRL 3-4 all the way up to about TRL 6-7 overall.

4. **Are you interested in physical RF or IR camouflage/shielding?**
   The short answer is yes. But the longer answer is that in this Collider's context, we're more interested in the digital or cyber domain for signature management.

5. **Does a current SBIR Phase 1 help in the Collider selection process?**
   Being a current SBIR is not part of the selection criteria. It might help for doing SBIR Phase III and things out in the future, but for this particular one, that's not part of the selection criteria.

6. **Can one company submit more than one capability?**
   Yes. No limitations.

7. **What is the Collider total funding budget as a program for this year?**
   It depends on how many good ideas we get. That's probably not the answer that you're looking for, but we have flexibility, anywhere from zero on up. It just depends on the quality of submissions that we get.

8. **OV1: C5I is a very large topic, could you provide some detailed use cases or operational vignettes?**
   Providing operational vignettes is a little tricky but you could definitely look at things like smart cities; how to digitally camouflage our operators and their equipment inside a smart city. When you start thinking about everything that could detect a person or things such as a Ring doorbell. If you walk past one of those, could that be turned into a sensor to detect not only a person there, but other actual equipment that the operator may have? You could also say multi-level security and tailorable encryption, those are top level when you start looking at that.
   Try to think in terms of where we are operating. That is incredibly broad since SOF is globally deployed. Obviously, we're supporting in Ukraine right now, but for smart cities like we mentioned or UTS (ubiquitous technical surveillance) environments, how do you operate in a highly sensed environment and still be able to hide? So that's tricky both in the digital domain like we mentioned earlier or in all physical operating domains, Ground, Air, Sea, and Space. What does that take to get a team in, get a team out, and make sure they're effective in operations? It is complex and multifaceted, but just try to think through the eyes of a team or an operator. How do we get into an area and make sure we are unsensed or make sure we can get to where we have to, without being picked up?

9. **Do you accept software-only solutions where we smartly encode the original data into a new format to conceal the real information?**
   Yes, we'd be interested in that. Devil is in the details with that one, but yes, we would be interested.

10. **Is autonomous re-supply an interest area for logistics? What is the operating profile of autonomous distribution platforms that would be most relevant to SOCOM**
    Yes, autonomous resupply is an area of interest. Specific operating profiles will be difficult to describe here mainly because they vary widely. We will say use your common sense, being able to move 10s to hundreds of poun ds of equipment over 10s to even hundreds of kilometers would be extremely beneficial to our operators. There is also a push towards using the space domain to pre-stage equipment and materials and then deliver those autonomously anywhere in the world quickly. You know what the physical operating domains are; we mentioned space, air, sea, and ground. But remember that SOF works through the services to in a lot of cases get

near or get to where they are going in part in terms of logistical supply. A SOF team is dependent on our service partners in moving stuff around. Big resupply vehicles, things of that sort would be out of the picture for SOF just because of that service element contingency. Think through the physical domains, what even a comprehensive, autonomous resupply chain would look like if that crossed, physical operating domains. Then also what would that look like from the service support side of things?

11. **What is expected/allowable cost share for Collider participation? Is ROM for participation only or can scope include development and demo implementation/build?**
    Expected cost share would be determined by which path forward. There are several different paths forward, including business to business partnering with SOFWERX, using another transaction authority which is the 4022 most likely, which does require cost share for anybody that's not considered nontraditional. Of course, cost share may also allow you to do a bigger project, so there's no real set on that. “Is the ROM for participation only or scope include development and demo implementation and build?” We're looking more for the overall/whole/complete project. In the submissions, include all aspects of it, including demo experimentation parts.

12. **Is there interest in reducing digital signature from an offensive perspective as well? Targeting/Analysis/etc?**
    Yes, absolutely. If you can hide your presence, and obfuscate that presence, then it produces your offensive attack space. Anything like that.

13. **Is LPD (Low probability of detection) radio technology development of interest to this collider or is there another forum for this work?**
    Collider's fine if you have a good idea definitely submit there. There are other pathways, S&T has broad agency announcement (BAA) that has one area that this would be relative to. But again, if you think you have something relative to what we're describing here, kind of the UTS you know, operations or operations in a UTS environment, then go ahead and submit through Collider.

14. **Can you explain the main differences between the Collider and Disrupter programs?**
    Collider, in the past has generally been a little bit higher TRL. Whereas the disruptor effort is more disruptive, breaking the laws of physics type of submissions. If you have an out of this world unseen capability, disruptor may be the more appropriate avenue.

15. **Do SOFWERX interests include wearables with meta materials technology?**
    I can't answer on behalf of SOFWERX, but in relation to Collider, the answer is yes. We would be interested in that, assuming the wearables with meta materials address the problem statements in this TFA. Also, all the spending that we do in S&T has to be SOF-Peculiar or SOF specific. So, if there's something that you think would be more service or conventional force applicable, we would say to leave that out. SOF has very specific mission sets that differentiate it from services. So, kind of thinking through that lens, is it SOF peculiar, is this relative to how SOF operates and

what we're doing?

16. **Are you interested in CI variants as well (i.e. identifying adversary use of similar techniques against our assets)**
    Absolutely. If we can identify similar techniques that an adversary would use, it helps obfuscate exactly what our signature is going to look like.

17. **Would you be interested in a "Waze for IoT" that tells operators what the local digital pattern of life is pre-deployment (and once in it?)**
    Yes, without having any more details than what is in that statement or question, yes, we would be interested in that. So, submit a white paper and we will get more details on it.

18. **Earlier you said that this TFA was not appropriate for physical (RF/IR) camouflage. But just now you said LPI/LPD waveforms were of interest. Can you elaborate?**
    The waveforms relative to whatever comms, communications devices, or radios that we're using is one element of being able to operate in a highly sensed environment. So, this is a complex, comprehensive picture. You have to think through multiple technology area lenses, in terms of creating a kind of holistic capabilities for SOF traditionally. Let's say the last 25 years or so we've been largely Middle East type operations. That's shifting to a lot more complex operating scenarios. The radio, or RF, elements are just one aspect. IR, or infrared, has very specific properties, and even within infrared are near, short, mid, and long wave infrared. They're very specific things that we have to, one be cognizant of but also two how do we overcome in just that range as well. When we say LPI/LPD waveforms that's specific to RF which would be specific to RF based communications, but that's only one aspect of a lot of elements figuring into this.

19. **Can the solution make the assumption that operators will have access to basic coms, internet etc, or does it have to include the full hardware package as well?**
    The hardware package in this case would say is largely dependent upon the solution set or capability set. Speaking in terms of should we make the assumptions, they're always going to have comms connectivity, Internet connectivity, largely where SOF is going to utilize the communications and data backhaul pathways that are available and very unique in a very unique sense as well. We may have comms connectivity at one point, or it may be contested, or we may be operating in a highly comms or RF congested environment which may impede communications pathways. It's not steady state in that there's inherent drop off at different points.

20. **Are you open to non-type 1 encryption solutions for multi-level security solutions? If the solution could eventually support type 1 would that be more desirable?**
    Yes and yes. Anybody that's in that communications field knows that there are different type 1 encryptions that can be used for other things and to talk with partners. So absolutely, we'd be very interested in looking at those solutions.

21. **Can you elaborate on "Joint and Partner information sharing" from Vignette 1? What Classification levels, interest in CSfC like applications as examples.**
    SOF operates heavily with our allied forces and partner forces and in some cases just even partner nations or host nations allowing us to operate to kind of within their confines. There's a lot of shortcomings on this front we would say right now, regarding addressing policy to

appropriately and safely be able to share info with joint or allied force as well as partner force. That's a tricky picture and largely is still a big sticking point right now, but a lot due to policy restrictions.

22. **Given the short timeline, will you be facilitating any teaming between submitters or gov't stakeholders that may have complementary capabilities?**
    Yes, across the board, kind of blanket answer on that. The specifics would be dependent upon what and how.

23. **Is there a funding ceiling for submissions that would immediately disqualify us from being down-selected?**
    No. We do have flexibility on this one.

24. **Will you be providing feedback on a rolling basis during submissions to refine potentially interesting solutions?**
    I do not believe that would be the intent. White papers can be submitted up until 22 March, that's when we will be reviewing the white papers.

25. **Can a training solution be proposed or purely technical widget?**
    Generally speaking we think of S&T as producing a widget, but we think if a training solution is proposed and is going to address the topic areas in this Collider, we think it would be considered yes. There are a lot of training needs now that are coming up relative to digital capabilities, cyber capabilities and all kind of going along the lines or related to the area of operations that we're describing this kind of smart city type UTS environment. We wouldn't rule out training related submissions. Definitely submit those as well.

26. **Is there any benefit or requirement to having a Vulcan scout card for submitted tech?**
    We don't know that this event actually has a requirement for it to be in Vulcan, but would say that the benefit is enormous because when you create that scout card in that database, there are hundreds, hundreds of other government agencies that can see that as well and then that affords them the opportunity to reach out directly to that submitter.
    In regards to this particular Collider event, there's no benefit or requirement detailed in the selection criteria. But overall, there's usually a benefit to having that in the that ecosystem.

27. **Regarding policy limitations for sharing between joint forces, is this a result of export controls or because joint forces do not support common encryption etc.**
    Yes to all. That's a kind of multifaceted picture there in terms of the export controls. Are we supplying say for instance, are we working with the partner nation or partner forces where we need to provide them some level of capability? And if say that capability is a radio, are we going to give them, is it going to have a different security field, different hardware aspect, but still be able to communicate with our radios? That's it. There's no easy button answer to that one. We think that's highly specific to like which tech, obviously export controls kind of vary across the board depending upon which country or countries that we're working with and don't support the common encryption etcetera. In terms of radios, that's a big sticking point is if we're using Type 1 encrypted devices, we can't openly or freely share those with partner force, partner nation type of situations. If it's with joint aspects even say service, service elements, you know that's a lot more open picture. If it's with say Five Eyes partners or our allies, that's a little bit

more free. It all boils down to the data-sharing aspects, which are largely policy-bound right now. A few different issues in that picture.

28. **Can you provide more info on the collider one-on-one sessions? Are they more like briefings or demos? Is there any coordination beforehand with attendees?**
    The one-on-ones will be exactly that, like coffee dates. The government stakeholder team will let SOFWERX know how long they want a brief and Q&A session with the selected vendor to be able to brief the capability that they submitted. Whether it is a demo or not will be up to the government stakeholder team and that information will be provided once downselects have been made. There will be either a virtual or in-person option for that is still to be determined. Yes, there will be coordination, you will be hearing from the SOFWERX Team, who will make sure that your team has everything that you need and that time slots and everything like that are solidified with the government stakeholder team before your one-on-one if you are selected.

29. **Is there any funding support for the demo/briefings?**
    There is funding to support possible follow-up awards and more information and details for that are at the bottom of the web page for Collider/Disrupter. The intention is to have selected organizations brief and then whoever is selected for possible follow-on awards will be announced during SOF Week at the Tampa Bay Convention Center. More details on funding for that portion will be provided directly to those who are selected for the follow-up award.
    Just to clarify, these organizations would be selected for a path forward which would depend on numerous different things including potential awards of an OTA or possibly B2B.

30. **If we are in prototyping, how close to FOC do we need to be for the demo?**
    Full Operation Capable. That's kind of a broad statement because you could look at that and say full operation capability, which means the next day you're ready to go implement right now, deployed. No, you don't have to be at that level. We do want to see proof of concept. There may be some refinement that might have to happen if such a project was selected down the road, but you always have to think about implementing it mass-wide enterprise-wide. You're going to need an ATO (authority-to-operate), anything that connects like that. There's a little bit more follow-up work that has to be done with that, but we really want to see that proof of concept. Can you prove that it works?

31. **For joint coms are you more interested in Edge Networks or enterprise style communication platforms?**
    The government is interested in both, however there is greater interest in Joint Communications that support operations at the Tactical Edge.

32. **Is the Government interested in hardware solutions for digital camouflage? Or does the Government define this as this strictly a software concept?**
    The government is interested in both hardware and/or software solutions to solve this broad challenge.

33. **Is there a minimum TRL level for the proposed technology?**

S&T efforts are usually between TRL 2-6. While there are no set parameters, Collider typically focuses on the higher end of that spectrum, while Disrupter would probably lean towards the lower end.