

Master Current Limitations

TEAM	Current Limitations	Ways to Overcome	
RED	Data - where do we get it, how much does it cost, who is buying it, is it part of the solution or is it outside	Raw and processed to avoid internal error - do not remove redundancy / and managed that data / tied to what you want to achieve / provenance	
RED	Integration of publically available information and private data		
RED	Data normalization and cleaning of text/unstructured data	Needs to be done at speed - does the shit quick	
RED	Data redundancy		
RED	Authorities, we can build stuff that they just aren't allowed to use in the first place		
RED	Rapidly evolving problem space, but similar systemic pace on acquisitions and events like this		
RED	Adoption of tools which already exist, or loss of tool use after commands pass on - possibly an issue of specialization into a singular method of solving a common problem		
RED	Training		
RED	Cost prohibitive, it isn't just buying inventory, it is buying a subscription, since pulling in data on a recurring basis and running these LLMs is expensive, these things tend to come with recurring fees which are a harder sell to the gov. at large		
RED	Acquisition authority is not placed in the hands of the people who require the tools themselves		
RED	There is a huge discrepancy between what people think they need - a match of their exact process, and the goals and actual needs of the system. This makes it hard to build for a small team, and then impossible to extrapolate to future teams which could use similar features.		
RED	Because there is such a quick turn over of problem sets in the military space that training and specialization is almost impossible to maintain		
RED	Trust, this is a new technology which we don't trust quite as much as a stackoverflow message, there is also a sort of data prov problem with LLMs in general		
RED	Saas is dying because it is so easy to build a dashboard app in a single day		
RED	Policy issues		
RED	duplicative data		
RED	acquisition timelines suck - not aligned to mission		
RED	storage of data		
RED	how to distinguish between best athlete		
RED	contract vehicles - how to innovate		
RED	operators do not have much say		
RED	funding Creta		
RED	lack of tradecraft		
RED	small company requirements no way to get your foot in the door		
RED	leadership removing roadblocks	MOE and ROI so that impact of decisions can be measured, ability to know what to message, and ability to see related issues.	
RED	risk aversion	Access to who can do what	
RED		Knowing how the series will land in the civilian population	
RED		Sampling of effect over time	
RED		Resonance of data	
RED		Testing - predeployment	
RED		Causal issues	
RED		Quantify MOE for leadership	
RED		At speed	
RED		Framed so leadership can understand	
RED		Define objective	
RED		Define Target Audience	
RED		Options to achieve objective	
RED		All data and tools need to be focused on the objective	
RED		Automating social science problems	
RED		Messaging targeted to the TA	
RED		Feedback on proposed actions	
RED		Linking kinetic action to the non-kinetic / and then targeted / blueprint for message	
ORANGE	Edge performance	Integration of data in legacy systems	
ORANGE	Data at the edge (data consistency)	Unified architecture for data access (API/MCP), infrastructure (containers/platforms/etc.)	
ORANGE	Lack of MOE	Containerized/portable applications	
ORANGE	Internal deconfliction	Increase pilots with end users to build solutions off of expertise	
ORANGE	Cross domain solution	Build systems that are grounded in doctrine	
ORANGE	DDIL	Build systems that have a direct operator-to-feedback pipeline for continuous development	
ORANGE	Fast sampling of target audience	Promote cross-domain solutions	

ORANGE	Data provenance	Inclusion of training tools/materials/documentation (interactive, i.e., AI assistance) inside of solutions	
ORANGE	Ontology rectification	Development of tools with continuous assessment capabilities	
ORANGE	target audience not social media	Platforms capable of ingesting multiple bespoke information sources	
ORANGE	centralized data / unification	FOCI compliant solutions for denied environments that involve hardware	
ORANGE	Training pipeline		
ORANGE	speed of adoption		
ORANGE	who talked to leadership first over tech analysis		
ORANGE	gov evaluation		
ORANGE	consistency in the chain of training and systems		
ORANGE	tool fatigue = too much glass		
ORANGE	Classifications = multiple levels		
ORANGE	Integration - open architecture / industry agreement		
ORANGE	Requisite knowledge of AI		
ORANGE	data retention		
ORANGE	bad data and no analysis		
ORANGE	prof dev models for ncso		
ORANGE	Data storage problems - we need a lot of data, but we aren't Google		
ORANGE	Data access problems - we need to be able to scrape all publically available information, but bot protections and regulations are getting stronger		
ORANGE	What does normalization for unstructured data look like? Is there a standard way to make sure that this works?		
ORANGE	Analysis bias via human moderation/selection bias - consider the data source selection problem, how are these sources chosen in the first place?		
ORANGE	Poor function integration - data scientists, social scientists, psyopers, and the command of psyopers all butt heads when developing this kind of approach		
ORANGE	Data interoperability across platforms		
ORANGE	Data processing pipeline transparency		
ORANGE	LLM hallucinations, unreliability, and evaluation		
ORANGE	How do we develop a system to check LLM claim validity against the current state of the world		
ORANGE	Tempo, how quickly can we ingest data? How quickly can we bring data to live? We need to inform live decisions.		
ORANGE	Shifting requirements		
ORANGE	Heavy time constraints - Psyopers need to be able to sit down for 3 hours and make a judgement, they can't spend all day on the problem like an analyst might		
ORANGE	Training - getting somebody up to speed and capable of making informed decisions		
ORANGE	How do we know what is actually resonant/important		
YELLOW	Unclear strategy	Data Pipeline Throughput, Common Ontology, Common Data Structure	
YELLOW	Classified versus unclassified information/data	Academics - Currently working a bit of each but building bespoke at this time GOTS	
YELLOW	Limited cultural expertise	Edge Theory - Common Location to process large volume of data and provide Process Data Agnostic	
YELLOW	Limited intelligence source	Virtual Investigations - Conduct data collection, through MA, push data to common data pipeline and then synthetic data creation	
YELLOW	Collect on the wrong thing	Opti Metrics - Social Media data pipeline, Data Enrichment, This is how you will process data, Synthetic Personas	
YELLOW	Lack of continuity	Shadow Dragon - OSINT Data at scale within SOCOM, Data Agnostic into data pipeline	
YELLOW	Expertise lacking in different modalities	Bad Monkey - Ontology Pub Sub and Agent Pug Sub	
YELLOW	Lack of interoperability	Omegas - PAI Company with AI system that produces reports, Language Agnostic, AI processes credibility of the source and if it was viable	
YELLOW	OSINT team lacks targeting expertise	Thorida - Data Collection and Data Analysis, COE of Data Pipelines and its Echolon, Modul First for Instruction	
YELLOW	Dependence on high-speed communications	perEdge Research - AI between data and events and grounding AI with valid of data Ground truth assessments and leads into training and war gaming. Academic Review of data, Validate Messaging, Validate Pipeline	
YELLOW	Lack of authorities on what can be collected	BabelStreet- Unstructure and Structured Data Analytics	
YELLOW	Speed of producing products/spontaneity		
YELLOW	Difficult to nominate civilians as part of targeting process		
YELLOW	How to engage target to get desired effect based on analysis		
YELLOW	Too many disparate platforms		
YELLOW	Cross domain solutions difficult		
YELLOW	Keeping current		
YELLOW	Training advance skills beyond the POQC		
YELLOW	Difficult to operate at the edge		
YELLOW	Educating beyond the basic information provided in institutions		

YELLOW	Partner nation tradecraft		
YELLOW	Limitations presented by whole of government vs military authorities		
YELLOW	Conflicting perspectives between DoS (other govt entities) and DoW		
YELLOW	Influence ops vs PSYOP		
YELLOW	Knowledge retention		
YELLOW	Learning from previous operations - applying lessons learned		
YELLOW	Authorities in distribution and dissemination: who engaging, controlling where messages go		
YELLOW	Complexity of tools		
YELLOW	Maintain pace of LSCO battle (BCTs, Divs, Corps): getting inside the targeting cycle		
YELLOW	Exercises not designed to exercise Competition, Crisis, Combat (fight)		
YELLOW	Maintain pace of LSCO battle for the Soldier		
YELLOW	How to communicate from mil to civ with CUI information		
YELLOW	Doctrine not keeping pace with realities of the battlespace (data collection)		
YELLOW	Rules for using Superior Intelligence (balance between machine and human)		
YELLOW	Not integrated into targeting correctly		
YELLOW	Inability to access populations not connected to the internet		
YELLOW	Inability to focus on the main effort (targeting process)		
YELLOW	Targeting WO		
YELLOW	Concentrate on lowest common denominator		
YELLOW	Manning structure too small		
YELLOW	Lack of interagency synchronization/deconfliction		
YELLOW	Spectacularly underfunded		
BLUE	Funding	We must be able to predict, defend, and list our ROI (this could be via MOE tracking and building the system into our projects in the first place), this makes all spending immediately defensible	cost scales with how we use and misuse tech, what are we actually measuring, we don't need to be using the best of the best LLMs for a bunch of stuff. It is difficult to sell a ROI for a lot of these products, perhaps we could look into building in visible ROI into our products. Indeed ROI can be grouped into a MOE metric, though I think we agree that MOE is something which is persistently hard to use. Since ROI cannot be measured in money - not a cooperation - we must use MOE to track the ROI in the first place. We must start with a forecasted MOE in the first place, which is explainable to an operator. An LLM might be able to walk through this process - predict an effect, take action, measure the real effect. This can remediate overuse, underuse, and various other problems as well. If MOE is a first class citizen in all tool usage
BLUE	First Sof Truth - Human Training Limitation	The burden of training and usage is on the product. This is solvable, do the UX, use AI to simplify. There are three levels of complexity - chat interface, dashboards, data platform - you may need to handle all three of these situations.	This is an industry problem first and foremost, the burden of the tool is on the training, the burden is on the government to ensure that the tool is easy to learn itself, we run into the issues of the people on the ground are more knowledgeable about the higher ups about the solution space. How does pricing run into training, it can be costly when you aren't excellent at using the system? We must design tools which minimize the cognitive load itself. We have to sell the product to both: easy to say that an insanely smart kid can handle the situation - throw them into hunger, conflicts, etc. and are they still able to learn the tools. Multiple levels of detail would be helpful - can people handle the high level (prompting and getting a response), the medium level (dashboards and findings), the low level (data, trends, etc.). The interface needs to be simple text because we need to be able to handle in KB/MB/GB all three levels.
BLUE	Lack of application of tools	See Funding. This is handled by MOE development.	
BLUE	Enabling individual to ask right questions to get what they need	See the discussion for training. There has always been a shortcoming in the training pipeline on the basic operator course side in "asking the right questions" - a revamp of this system would be helpful.	This should be handled in the basic operator course, not necessarily industry responsibility.
BLUE	Focus on wants and define the problem	See Funding. This is handled by MOE development.	
BLUE	Data Silos		
BLUE	Buy in for everyone to use the same system		
BLUE	Risk averse to sharing data/IP		
BLUE	Interoperability, common data analytic formats		
BLUE	Validation and comparison of tools		
BLUE	Social science theory, how to predict transitions across the 7 steps		
BLUE	Measures of effectiveness, how to measure outcomes and behavior	See funding. This is a proactive process. You must predict, monitor, and then list effects.	
BLUE	Volume / brute force versus targeted interventions, operational philosophy	Build scalable technology. You should be able to handle both single posts and full campaigns.	we don't get to chose, psyopers don't get to chose, that decision is chosen much above this domain
BLUE	Bounded autonomy, what level of approval	Develop policy which defines which decisions may be made by Psyopers.	who your approval authority is is predefined and different across different clients
BLUE	Partition of models across contexts, large and small, generative and discriminant	Don't throw GPT-6 at summarization. Handle this yourself.	
BLUE	Compute resources, local vs. proprietary models	This can be solved yourself. Do the training and the cost comps, both are useful.	
BLUE	How to marry kinetic and non-kinetic interventions	Predictive analysis can inform these decisions based off MOE, leading to kinetic action being informed by non-kinetic ROI	it is always easier in the moment to handle a situation kinetically, it may not have the intended OR better MOE
BLUE	Where to have human control, where to defer to AI	Develop policy which defines which decisions may be made by LLMs.	This should be handled in the basic operator course, not necessarily industry responsibility
BLUE	Reactive vs. proactive operations, how can AI facilitate	Develop policy which defines which decisions may be made by LLMs.	
BLUE	Attribution of adversarial efforts across large data volumes		
PURPLE	Disparate Systems (not interacting/feeding into each other)		
PURPLE	SOCOM PsyOps -> tactical operator (closed infrastructure)		
PURPLE	Over-reliance on Public Information/scrapers (need to ground in reality)		

PURPLE	Meet the user where they are (commander vs analyst)		
PURPLE	Limited access to closed groups		
PURPLE	Tempo is faster than we are aggregating/acting		
PURPLE	AI is unreliable (general knowledge and confidently wrong)		
PURPLE	Approval for messaging is too slow (we're reacting way late)		
PURPLE	Area of Effect of messaging is hard to gauge		
PURPLE	Lack of knowledge of what authority you have		
PURPLE	We don't have good tools for messaging that are targetted and approved		
PURPLE	Measuring effectiveness of interventions		
PURPLE	Training required		
PURPLE	Raw data access, don't need analytical layer		
PURPLE	Unified data lake; e.g. an analogous solution to DIA's planned ontologies		
PURPLE	RAG and underlying ground truth to products		
PURPLE	Disparate ontologies		
PURPLE	Synthetic data, inaccurate data		
PURPLE	Imperfection of target audience or mission models		
PURPLE	Instrumentation for risk and effects of messages; what is anticipated blast radius for a message? Everything turns high risk		
PURPLE	State estimation of effects, evolution of unfolding and changing IE. Rapid changes in environment		
PURPLE	Approval timelines for products		
PURPLE	Trust barriers and deterministic guardrails for LLMs and technologies		
PURPLE	*Tiered trust barriers for different risk levels and scenarios		
PURPLE	Perceived risk of information operations, unknowns create low risk tolerance		
PURPLE	DDIL environments, cloud vs. downrange equipment (at the edge)		
PURPLE	Avoidance of adoption due to limitations, knowledge that materiel is substandard w.r.t. industry		
PURPLE	Ruggedizing		
PURPLE	Interoperability, open APIs, unified data models, agnostic to data and hardware environments. Workflows should be continuous no matter where you are		
PURPLE	Forward and backward interoperability, e.g. being able to fold in old AND new capabilities		
PURPLE	Disparate silos of requirements. Five PMs at SOCOM who touch one level of requirements, but the rest are left under-resourced		
PURPLE	Territorialism of resource allocation and programs		
PURPLE	Cross-domain access, CDS, should work from unclass dirty/CUI/S/TS		
PURPLE	Overclassification too soon		
PURPLE	IO happens in an unclass world. Orders and missions are HS		
PURPLE	Access control: users accessing restricted content or user-based access control is a gap		
PURPLE	LLM agent access control as a future problem		
PURPLE	Model dependencies, model access controls. One big model running on a server vs. smaller models running on different systems, every layer further complicates control rules		
PURPLE	Compute power: token use, token bills when VC money stops subsidizing. Discounts won't last, are heavy to US government right now. Tokens vs. joules		
PURPLE	Surfacing value added for investments, especially around AI usage. Individualized token budgets		
PURPLE			
PURPLE	Limitation/Problem Buckets	Solutions	
PURPLE	Authority/Permissions/Education	Policy/UCP/Strategy dumped into a system (RAG), who do we need to follow up with	
PURPLE	Unified platform (across echelons)	Planning-Analysis/Production/Post-Production-Analysis (small solutions for each, wrap it together)	
PURPLE	Risk/Risk Mitigation Articulation (Willingness to exercise)	Currently, senior person pokes holes until its ready to put before leadership	
PURPLE	Training/Tech Adoption (Commander visualization)	Platform based on role, LLMs to mediate data presentations to different levels	
PURPLE	Data collection/Aggregation/Unification (where does this live)	Collection is weighted locally and different mediums (PAI aggregation vs personal text/social media), data enrichment	
PURPLE	Veracity/Guardrails/Measurement/Validation	Levels of access (run on a computer, vs larger models, vs simulations)	
PURPLE	Where/How We're Getting Data (Information Space)	Generate ground truth by active data collection (getting lowest level person the ability to collect data is our top priority)	
PURPLE	Tempo	AI augmentation, collect early/often so context is present, automating authority process	
WHITE	Insufficient data infrastructure	set standards at enterprise level	
WHITE	Training/technological literacy	DOTMLPF	
WHITE	Lack of unified requirements/demand sets	single repository of all requirement documents	
WHITE	Acquisition timelines mismatched to force cycle	first define reqs, then use ai to summarize and humans to va;date	

WHITE	Platforms lack interoperability	published requirements for architecture	
WHITE	Staff technical capability/literacy	advanced training pipeline (personalized)	
WHITE	Requirement generation and validation process too long	use agentic ai to overcome funding and manpower limitations	
WHITE	Intermittent/unreliable funding streams	establish the program of record	
WHITE	Concentrated contract streams/systems integrators	we need defined AI stack requirement not system integrators	
WHITE	Authorities piece is backwards / pre authorization	speed up approval processes	
WHITE	Lack of measure of effectiveness as to the target population	it is on the planner to define the MOEs	
WHITE	Leadership challenge	HITL and what risk the commander can accept; how do we build trust between the commander and autonomy	
WHITE	ROI on IO effectiveness	commanders have different ideas on the MOEs	
WHITE	ROI and impact on funding	establish the program of record	
WHITE	Authorities and MOE / ROI relationship	let the commander and his planner define their MOEs	
WHITE	Alignment of commander's intent and kinetic effect	things we do in the kinnetic domain inform IO activities and we need to tie it together	
WHITE	Sentiment is not predictive	clarity for where analytics fit within doctrinal	
WHITE	Disorganized authority structure creates friction	be proactive about it	
WHITE	Belief structure mapping	LLM is a partial solution, they can be aligned across cultures, but it has to be continuous	
WHITE	Speed of decisions	ai and agentic ai autonomy	
WHITE	Commander eduction consistency / interp	every commander should have a personal ai assistant that trains him continuously	
WHITE	comfort at the speed of operations	they are different operations and the same tools should not be used for tactical vs. strategic	
WHITE	Fear of unintended consequences	Risk managed training / leverage AI to identify risk	
WHITE	credibility of capability	Validation tools have tpo be developed; all vandors should be evaluated using an apple to apple comparison	
WHITE	Lack of technology coherence	this is actualy to your advantage; tools trained on different data and with different models can tell you more when they agree and disagree	
WHITE	tacit knowledge is lost between operations	preventing knowledge loss using ai	
WHITE	training is still whitecarded	ai tools that allow rapid injects and measure synthetic audience effects	
WHITE	narrative intelligence tools are mostly text based	invest in multimodal ai - image and video product generation	
WHITE	most if ai tools are LLM and they are not validated	develop a unified ai validation ecodytem that will enable apple to apple comparison across tools	
WHITE	the lack of measures of effectiveness of autonomy and automation within the IO cycle'	how to you measure the effectiveness of a human vs. ai automation vs. autonomy vs. human + ai in the IO workflows	
WHITE	many toll can't cross classification boundaries	local models pretrained on operational data	
WHITE	how do you evaluate ai tools and how they are not doctrinally aligned	focusing ai adoption on doctrinally consisten across fyncions, roles, workflows	
TEAL	lack of a unified government platform to do the 7-step process	Clustered SLMs	
TEAL	insufficient data	Tooling	
TEAL	Disparate/uneven tool-sets	Specialized Models to return fit (Measure of effectiveness)	
TEAL	lack of "economies of motion"	Appropriate assessment plan	
TEAL	the lack of unified design philosophy	miro (betting 10000 agents)	
TEAL	what should be automated versus what should a human do	standardization and knowledge of tools	
TEAL	what type of technological tool - GenAI versus algorithms versus multi-modal models	research automation	
TEAL	lack of validation for AI tools	agentic system with tooling; orchestra and swarm - validation of each tool/output in every tool of the workflow	
TEAL	lack of evaluation tools	mirofish clustered slms (more agents higher accuracy)	
TEAL	lack of understanding what use-cases are even appropriate for what tools to begin with	access to previous data of MoE and MoP for training/validating solutions	
TEAL	knowledge gap between user and industry	rl simulated environments of operations	
TEAL	open-source vs. proprietary models	auditability	
TEAL	over-coming cultural biases	human on the loop	
TEAL	our adversaries have achieved autonomy of influence operations	ai detection + reverse image search (may be OSINT)	
TEAL	Influence operations have to comply with so many different authorities, both within DoW and DOS	geographic linking to posts and social media	
TEAL	lack of object-based intelligence	main blocker: bereaucracy, lack of data. Technical solution: agentic system with tools listed above, possible multiple supervisor agents.	
TEAL	lack of known-requirements	more communication between orgs	
TEAL	so many disparate streams of media data (and they're expensive)	some tools fully autonomous (i.e. defense)	
TEAL	offline ai models vs edge (requires server)	source of the manipulation (provenance)	
TEAL	resource constrained environment (signal, compute, hardware)	more communication between orgs with disparate requirements (	
TEAL	level of structured vs unstructured data	data cataloguing & standardizatio	
TEAL	multimodal vs not, language vs not		
TEAL	hyperscaled individual personality simulation		
TEAL	bereaucracy		
TEAL	autonomy vs control/ kill switch		
TEAL	intelligence reporting vs		
TEAL	manifestation of physical data/motions		
TEAL	classification issues		
TEAL	geospatial imagery		
TEAL	generalist		

TEAL	2 weeks for intense research - target audience, fence sitter		
TEAL	better measure of performance/effectiveness		
TEAL	manual assessments		
TEAL	science limitation: system is only as strong as the weakest tool link		
TEAL	finding originator of disinformation		
TEAL	data sharing across orgs		
TEAL	curse of knowledge		