Cyber

Theme	Area of Interest	Rationale
Cy.1 Defensive Cyber Operations (DCO)	Cy.1.a Secure / Resilience by Design	Establish secure foundation for cyber operation with system with reduced attack surfaces.
	Cy.1.b ICS/SCADA	Establish protection of Internet of Things (IoT) which affects infrastructure of and support to friendly forces.
	Cy.1.c RF	Enable friendly Cyber over RF and detect and identify Cyber actors' use as well.
	Cy.1.d Other non-IP related terrain	Understand sources and be able to defend against Cyber actors using non-IP related terrain.
	Cy.1.e Other non-IP related terrain: Red AI effects on Blue AI	How do we ensure Blue AI isn't "poisoned" with an adversary's agenda?
Cy.2 Offensive Cyber Operations (OCO)	Cy.2.a Human-machine partnering to generate packages applicable to current opportunities	Be prepared to engage Cyber actors via current and emerging opportunities despite dynamic changes – automated AI probing of adversary systems builds, in collaboration with humans, packages ready for OCO.
	Cy.2.b Identify and track Targets of Interest (ToIs)	Integrate with existing Cyber platforms to provide capabilities to detect, identify, and geolocate ToIs in Cyber and physical domains.
	Cy.2.c Cyber power projection	Vast array of Deny, Delay, Disrupt, Destroy, and Manipulate (D4M) effects across a multitude of cyber targets
	Cy.2.d Operations in the Information Environment	Integration between Cyber and Information Warfare
Cy.3 Cyber Command & Control (C2)	Cy.3.a Cyber C2 for "web kill" mechanism	How a Cyber weapon can be called upon, either planned or dynamic, by another domain to generate effects through establishment of common data formats across Joint systems such that cross-domain data sharing in find, fix, track, target, engage, assess (F2T2EA) process results in the same ID on the same target across domains, providing a web kill mechanism – enables Joint All Domain Command & Control (JADC2).
	Cy.3.b Integrated multidomain effects	JADC2 – coupling multi-domain effects in order to create convergence of mass on target (may be related to Cyber C2 for "web kill" mechanism)
Cy.4 Cyber ISR	Cy.4.a Predictive non-Traditional Intel from Cyber	Empower human decision makers with ongoing AI monitoring of world leaders and world events such that machine learning refines its ability over time to predict unfolding events in next 24 hrs and beyond. Relegate analytic crunching to computers and enable humans to make informed "human" decisions – AI doesn't tire and can monitor 24/7/365, producing correlations and projections from massive data that humans could easily overlook.
	Cy.4.b Cyber Analytics -- actionable, decision quality information	Techniques to determine what data is essential amidst big data in order to successfully accomplish mission objectives, while avoiding looking at the "wrong" data / distractors when lives are on the line. Perform essential Cyber and non-Cyber Intel integration.
	Cy.4.c Media trust and forensics in non-traditional Intel sources	H.R.3600 - Deepfakes Report Act of 2019 requires, in consultation with SECDEF, the Science and Technology Directorate in the Department of Homeland Security to report at specified intervals on the state of digital content forgery technology. Aids in situational awareness – need to generate actions to real events, not get played with elaborate deepfake distractions.