Information Maneuver
Live, Virtual, Constructive – Training Environment (LVC-TE)

I/ITSEC Brief

Col Adam Bryson
IEBA Project Lead
adam.bryson@usmc.mil
240-761-2101

This Briefing is **UNCLASSIFIED**

CAO 21 Nov 2024

Information Maneuver Training Gap

DC I is the LVC-TE / MCTE stakeholder for Information

- Legacy Terms: Cyber, EW, Networks
- Information Doctrinal Terms: Information Advantage – Systems Overmatch, Prevailing Narrative, Force Resiliency
- Gap: Information Maneuver Training System

Information Advantage – exploitable condition resulting from one actor's ability to generate, preserve, deny, and project information more effectively than another. Marines seek to create and exploit three types of information advantage: systems overmatch, prevailing narrative, and force resiliency, along with other decision, temporal, spatial, or psychological advantages— through rapid, flexible, and opportunistic maneuver. (MCDP 8, 21 Jun 2022)

Current State: ad-hoc OJT on commercial tools
Deficiencies
• Information maneuver in exercises (tiers 1-3, wargames, TTXs)
• Information advantage in competition (PH 0/1) training opportunities
• Information models for Information mission rehearsals and realistic wargaming

Desired Future State: Information integrated into training
Solutions
• Navy/Marine Corps, Army partner on Information LVC-TE
• MCWL exercise design incorporate MCWP 8-10 frameworks
• Incorporate training with service schools and PME
• Cross functional training for Intel to support Information

JLVC Information Model Development

- Information Advantage is an exploitable condition which can be measured
- Information Maneuver sets conditions in competition for crisis/conflict (also measurable)
- ONR & DEVCOM submitted proposal to develop and deliver JS J7 the live, virtual, and constructive training environment (LVC-TE) for Information by 2026
- **ONR Project OMEN** provides API and common data model for Prevailing Narrative (i.e. cognitive human-dimension)
- **DEVCOM CyberBoss** provides API and common data model for Systems Overmatch and Force Resiliency in training (i.e. Cyber, EW, and Space)

JLVC Information Model for joint forces to conduct Information maneuver rehearsals and fully integrate Information into all-domain maneuver in exercises and wargames

Information Advantage

Systems Overmatch Technical advantage of one side over another yielding fires, intelligence, mobility, logistics, or command and control advantages.	**Generate**	Build situational awareness, gain access to the opponent's information and systems, develop plans and orders, obtain permissions.
	Preserve	Prevent an opponent from accessing, manipulating, or destroying friendly information; guard against internal threats.
	Deny	Defeat or disrupt the opponent's ability to gather, make sense of, or use information.
	Project	Manipulate, corrupt, or deceive the opponent's sensors, systems, human-machine interfaces, and computer processing.
Prevailing Narrative Public opinion or perception advantage of one side over another, yielding trust, credibility, or believability.	**Generate**	Build understanding of key pre-existing and potential narratives (friendly, neutral, opponent) to include all relevant contexts and nuances.
	Preserve	Protect and defend the friendly narrative from opponent disruption and replacement; document and maintain unit histories and historical events with accuracy.
	Deny	Deny the opponent's ability to effectively communicate their narrative.
	Project	Communicate the friendly narrative by coordinating and synchronizing all communication, messaging, and actions, nesting them within the strategic and joint force narratives.

Marines apply our maneuver warfare philosophy to gain and maximize advantages over competitors or adversaries. Information advantage is an exploitable condition resulting from one actor's ability to generate, preserve, deny, and project information more effectively than another.

Force Resiliency Ability to resist and prevail against adversary technical disruptions that malign activities (disinformation and propaganda).	**Generate**	Build understanding of own force information vulnerabilities, actual and potential threats; identify risks and opportunities for action.
	Preserve	Recover from opponent information disruptions (functional or cognitive); educate and train against cognitive biases; conduct robust media literacy training.
	Deny	Defeat or disrupt the opponent's ability to access, gather, make sense of, or use information; guard against cognitive biases, conduct media literacy training to ensure Marines recognize and stop foreign influence.
	Project	Manipulate, corrupt, or deceive the opponent; communicate by action (exercises, demonstrations, freedom of navigation operations) to reassure allies and partners and send deterring messages of resolve to actual or potential adversaries.

MCDP 8 – Information, Table 3-1. Information Advantages and the Functions of Information

Information Maneuver

Generate, Preserve, Deny, Project

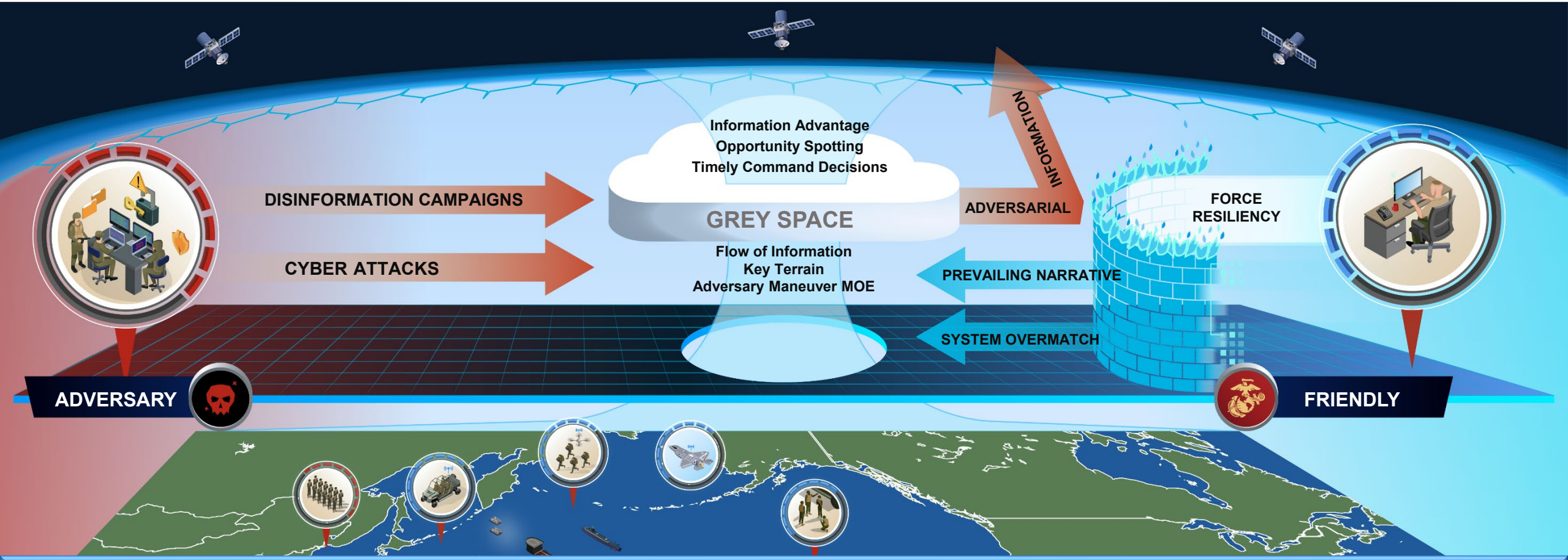
Information maneuver shares core principles with traditional maneuver warfare, emphasizing position and movement over brute force. Both aim to disrupt, disorient, and exploit vulnerabilities in an opponent's forces or strategy, whether on the physical battlefield or within the informational landscape.

- **Maximizing Flexibility and Adaptability**: Information maneuver requires a dynamic approach to managing and distributing information, rapidly responding to emerging narratives, misinformation, or changes in the public sentiment.
- **Seeking Psychological Advantage**: Maneuver warfare often aims to exploit the psychological impact of unexpected or unpredictable military actions. Similarly, information maneuver targets the cognitive domain, seeking to influence perceptions, attitudes, and behaviors through strategic communication efforts. This can involve shaping narratives, pre-empting misinformation, and psychologically dominating the information space to demoralize the opponent and garner public support.
- **Exploiting Weaknesses**: In traditional maneuver warfare, forces aim to identify and exploit gaps or weaknesses in enemy defenses. Information maneuver similarly looks for vulnerabilities in the information space, such as credibility gaps or divisive issues, to introduce narratives that can create confusion, sow discord, or shift public opinion in a favorable direction.
- **Focusing on Speed and Surprise**: Speed and surprise are hallmarks of effective maneuver warfare, as they complicate the enemy's decision-making processes. In the realm of information, speed refers to the rapid dissemination of narratives and counter-narratives, while surprise can involve unveiling unexpected information or revelations that reshape the public discourse.
- **Integrating Multi-Domain Operations**: Just as modern maneuver warfare integrates air, land, sea, and cyber domains, information maneuver integrates with other operational domains to achieve synergistic effects. Information operations can prepare the environment for kinetic actions or mitigate the fallout from physical operations through strategic messaging and narrative control.
- **Objective-Oriented**: Both forms of warfare are highly objective-oriented, though their goals might differ. Traditional maneuver warfare might aim for territorial gains or the destruction of enemy forces, while information maneuver aims to win hearts and minds, control the narrative, or manage public perception both domestically and globally.

Information maneuver is an extension of the principles of maneuver warfare into the cognitive and informational domains, where battles are not fought with physical weapons but with data, narratives, and influence. Both forms of warfare require agility, strategic thinking, and an acute understanding of the opponent's vulnerabilities and intentions.

Assessing Information Maneuver

Information Environment Battlespace Awareness – the integration and application of all relevant information about the IE to provide a running estimate of threats, vulnerabilities, and opportunities across all dimensions of the IE. **(MCO 3500.26B, 15 Jul 2022)**



IEBA assesses Information maneuver by bringing Information expertise to support the IPB process. Information maneuver is an extension of the principles of maneuver warfare into the cognitive and informational domains, where battles are not fought with physical weapons but with data, narratives, and influence. Both require agility, strategic thinking, and an acute understanding of the opponent's vulnerabilities and intentions.

PRIME: Persistent Range Information Maneuver Exercises

- **OBJECTIVE:** PRIME will provide the Joint community with an All-Domain Information Environment and Cyber / Non-Kinetic Effects warfare training, experimentation, and analysis capability, integrated with kinetic DoD simulations, enabling All-Domain readiness. This will provide a range to conduct and assess Information and Cyber Maneuvers to create and exploit Information Advantages that accurately represents the aspects of the Information Environment.
- **Use Cases include exercises involving:**
  - **Information Maneuver:** depicting how friendly, adversary, and neutral forces observe, orient, decide, and act on information IOT analyze and visualize IE to plan and conduct Information activities to exploit opportunities and protect vulnerabilities.
  - **Cyber Operations:** Cyber attack, defense, and mitigation.
  - **All Domain Operations:** training environment with land, maritime, air, space, and cyberspace domains; the information environment; and electromagnetic environment represented.

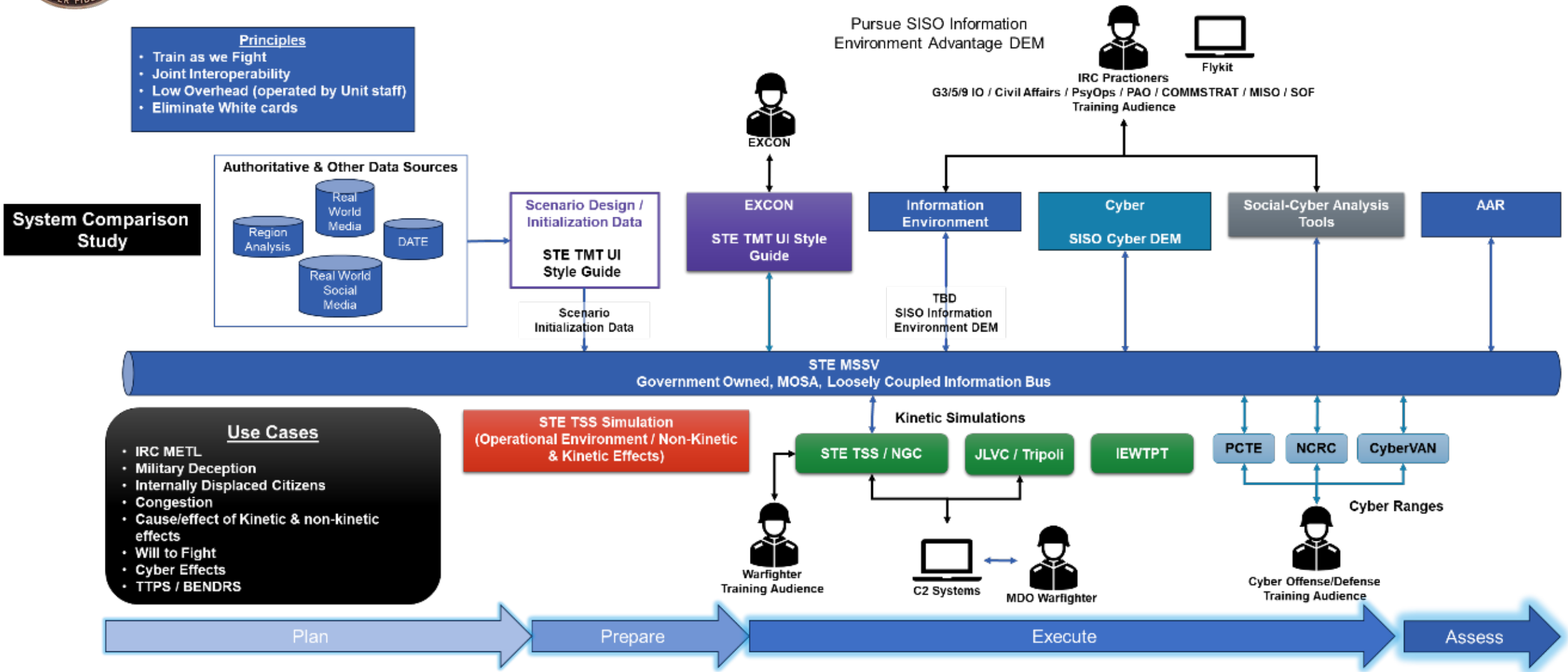
- **Description of solution:** Integration of the Synthetic Training Environment (STE) / Next Generation Constructive (NGC) / JLVC with existing Operational Information Environment and Cyber tools to provide new All-Domain / Multi-Domain Operations (MDO) training, experimentation, and analysis capabilities.
- **JLVC Modernization Capability Drivers: 1, 2, 3, 6, 8**
- **FY26 JOTG: 1, 2, 3, 4, 5, 6, 8**
- **Contribution to Joint Training:** These capabilities will enable exercise planners, white cell adjudicators and exercise managers to create, monitor, and dynamically adjust realistic information maneuver at scale that provide experiential learning and realistic simulation, with daily assessment of warfighter performance in full spectrum information warfare scenarios such that trainees are using the same tools they would use in the field.

- **Key Partners/Participants:** Navy (ONR, NAWCTSD), Army (DEVCOM), Marines (DC-I)
- **Key Deliverables:**
  - Synthetic Training Environment (STE) / NGC / JLVC integration
  - Integrated Information Maneuver range
  - AI-assisted scenario & synthetic data creation & visualization system for all-domain information warfare that includes at scale disinformation, inauthentic actors, adaptive personae & audience, cyber attacks, cyber & cognitive effects & dynamic response
  - Integrated data driven audience and persona models to increase scenario & social media accuracy vis-à-vis contested areas
  - Propose enterprise level data standards for information maneuvers (e.g., cyber, social-media and media)
  - AI-scenario and synthetic data generators, accuracy guarantees for synthetic data, TTPs for information maneuvers, assessment metrics
  - White-cell dashboard for near real time assessment, management, and command support for operations in the information environment
  - Leadership and communicator guidance tools for course of action planning as part of an exercise OODA Loop.

- **CTF Training Gap Linkages: A&P Integration, Data Sharing**

- **Key Milestones:**
- Annual International Limited Objective Experiment with FVEYS & Coalition
- Option: Embedding in Joint Exercises Annually (1-2/year) to include international exercises (.5M per exercise)

PRIME Overview



Backup Slides

IEBA Current State (Feb 2024)

Doctrine for IEBA is set, but detailed guidance pending. Gaps exist in organizational IEBA roles, with USCYBERCOM's partial coverage and no entity for Prevailing Narratives. IEBA training relies on ad-hoc commercial tool use, with DoD exercise integration needing improvement. Some tool standardization, ARCHER faces funding issues.

- **Doctrine**: MCDP 8 and MCWP 8-10; JP 3-04 but CJCSM 3212.01 has not been updated since 2010. The JOPTIK TTP (Information Maneuver) at JIOWC but not yet integrated in doctrine.
- **Organization**: Undefined IEBA requirement at echelon.
  - Strategic – No FCC for Information. USCYBERCOM for SO and portions of FR. No organization for PN.
  - Operational – Service-retained MCIC not fully staffed or funded. MARFORs not staffed or funded (ad-hoc, O&M, CTR-dependent).
  - Tactical – MIGs not fully staffed/funded (ad-hoc, O&M), no standard Information detachment with I-ISR/I-OPE prior to deployment.
- **Training**: ad-hoc OJT on boutique commercial tools. Deficiencies: 1) Information in DOD exercises (tiers 1-3, wargames, TTXs), 2) competition (PH 0/1) exercises for GPC missions; 3) Information models for Info Adv mission rehearsals and realistic wargaming.
- **Materiel**: Decrypt, Pulse, C2IE increased usage, ARCHER program (funding profile and FY25 funding gap). Deficiencies: 1) Info Adv ADS identified; 2) IE-COP requirement codified and resourced.

IEBA Current State (Feb 2024)

The lack of specialized ranges impedes leadership's IEBA utilization for decision-making, amid a broader expertise deficit across all levels. Policy progress is slow, forces await official plans or tasking to fully operationalize IEBA.

- **Leadership and Education**: Lack of Information ranges and wargames to educate leadership on the complexities of the information environment and how to leverage IEBA to make informed decisions and drive operations.
- **Personnel**: Operational and Intelligence expertise lacking for IEBA at every organizational level (ad-hoc, O&M, CTR-dependent)
- **Facilities**: Developing facilities that can support the advanced technological requirements of IEBA, including secure and resilient communications and data processing centers.
- **Policy**: Service-retained forces require PP&O Service Plan or GFM tasking for Information authorities. No PAI SECNAVINST to complement OSINT SECNAVINST to cover how PAI is used for use cases other than intelligence (PM ICO requirement to resource tools to OPFOR that use PAI for anything other than intelligence).

IEBA Desired Future State

MCRPs developed for IEBA and Information Maneuver. Define staff IEBA roles and implement MKG and C2IE standard across orgs, Information tasks for Service-retained forces. Incorporate MCWP 8-10 into training, develop Information Maneuver training, JS J7 OPR for JLVC Information model with MCIC, OPNAV N2N6 and JIOWC. ARCHER baseline and hub phases to standardize tools.

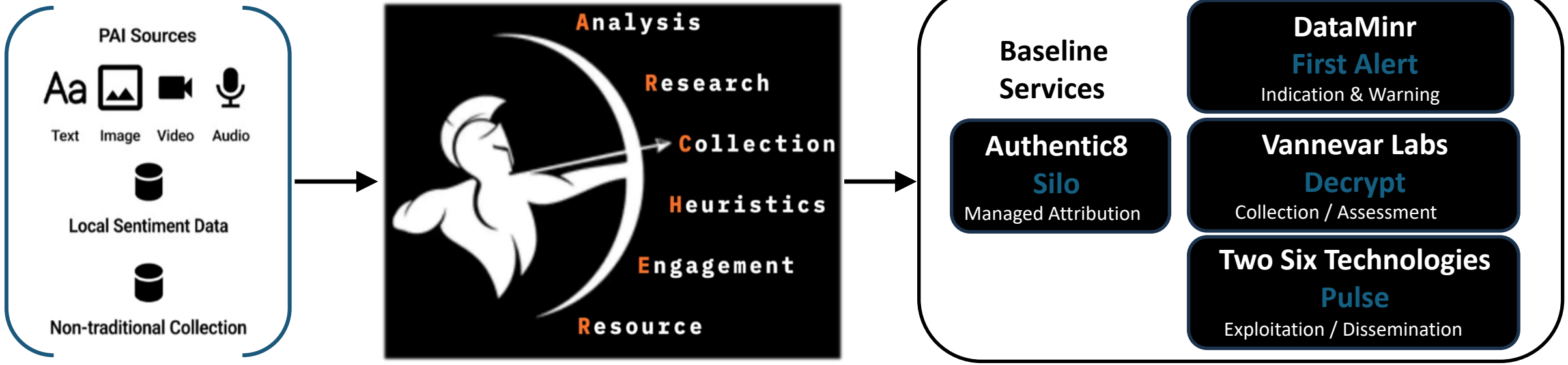
- **Doctrine**: Develop MCRP 8-10.1C Communication Strategy Research & Assessment, Develop MCRP 8-10A for Information Maneuver using JOPTIK TTP, formalize a Communication Synchronization process, develop C2IE COI
- **Organization**: Review and define staff organizations/units of action responsible for PN IEBA (MEF AC/S G7, MIG, MIC, etc.), develop a threat and plan informed concept for Communication Synchronization entity, implement enterprise MKG and C2IE standards, seek PP&O Service Plan or GFM tasking for Information authorities for Service-retained forces
- **Training**: MCWL exercise design to incorporate MCWP 8-10 IEBA framework(s), review/refine MAGTF T&R to incorporate PN IEBA and MOP/MOE development standards, incorporate IEBA and PN within service schools and PME (NIU), cross functional training for 02XX to support MISO/COMMSTRAT, Navy/Marine Corps partnership as JLVC Info model OPR - build model w/ MCIC, ONR OMEN, SOCOM SITE, and UMD ARLIS, Information Maneuver Training, JLVC Information model validation beginning at MWX 5-24
- **Materiel**: Requirements for IEBA with CD&I Gap #G245 for funded program of record for IEBA, tool interoperability with other JIIM organizations (DoS, DHS, etc.), ARCHER (PAI Tools) – MDAP AAP program transitioned to SWP, contracting by PM ICO and PEO LS, enterprise licensing by PM ICO with PEO Digital and vendors (VL, TST, Authetic8, DataMinr). Training will be a contract deliverable. NIWC-A and SDO with Microsoft to provision IMDF MLZ to host ARCHER Hub in 90 days once funded

IEBA Desired Future State

Information Maneuver demonstrated on JLVC Information model at future war games. MOS training on IEBA and Information Maneuver, fence Info Forces and increase security clearances. PP&O or GFM tasking for Service-retained forces to conduct IEBA. Define Operational use of PAI with ATSD PLCT and OUSD-P to close policy gap.

- **Leadership and Education**: Information Maneuver demonstrated on JLVC Information model at war games to educate leadership
- **Personnel**: Review/refine MOS(s) capable of PN IEBA (4505, 0231, 17XX), Fence Info Force(s) to priorities efforts in the IE, develop cross-functional R&A teams including linguists, increase security clearances of those responsible for narrative R&A, account for contractor (FTEs) providing IEBA expertise.
- **Facilities**: Developing facilities that can support the advanced technological requirements of IEBA, including secure and resilient communications and data processing centers.
- **Policy**: Clearly define operational use of PAI with ATSD PLCT on draft CAI/PAI DTM and OUSD-P on SOIE I-Plan. Establish working group and community of practice for OIE. Draft MCO for PAI ISO OIE.

ARCHER Baseline: Software as a Service



Silo is a managed attribution platform that **enables full use of the web without risk of exploit, data leak or resource misuse.**
First Alert is an I&W platform that **transforms PAI into actionable alerts, identify the most relevant information in real time.**
Decrypt is a data fusion platform that **collects and analyzes hard-to-access foreign sources.**
Pulse is an information dissemination platform that **provides services to automate delivery of content.**

Software as a Service (SaaS) is a method of software delivery and licensing in which software is accessed online via a subscription rather than bought and installed on individual computers.

Information Maneuver Services for Information Advantage

Information Maneuver Range at SLTE 5-24

Planning Tools

AESOP
Scenario Creator

Carnegie Mellon University
Netanomics

SITE ICS

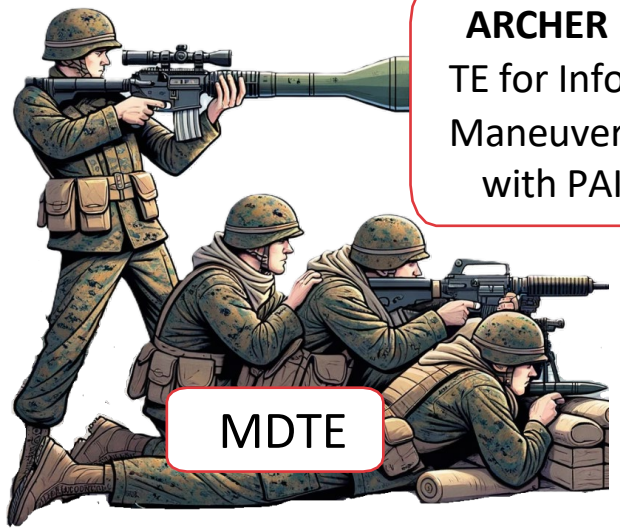
Visualization Tools

SITE ICS

ORA-Pro
Models & Tools

Netanomics
Carnegie Mellon University
Blue Halo

ARCHER



ARCHER
TE for Info Maneuver with PAI

MDTE

Analysis Tools

MOMUS
LLM Validation

Netanomics
Soartech
Blue Halo

SITE ICS

SITE

Synthetic Environments

ARLIS
ICS

Audiences

Exercise Assessment Capabilities

Soartech
Cognitive Performance Group
MIT-LL

SITE ICS

MOE Tools

Griot and SceneGen LLMs

Soartech
Blue Halo

SITE ICS

Content Generators

SLTE 5-24 AAR

- First exercise with an information training range
- After 36-hour training block the Multi-Domain Task Element (MDTE) could identify prevailing narratives and information maneuver threats, provide alerts and develop targets, all within the synthetic information environment (IE)
- Synthetic IE built in three days with exercise control aligned with exercise objectives including MSEL sync matrix
- 42 tasks identified to fully develop Information LVC-TE for PN, SO and FR training

Information Environment Battlespace Awareness

- Information Environment Battlespace Awareness (IEBA) refers to the understanding and insight into the information environment within a specific operational area. The information environment encompasses all the individuals, organizations, and systems that collect, process, disseminate, or act on information. It includes physical, virtual, and cognitive dimensions.
- In a military context, battlespace awareness involves the comprehension of the operational environment, including adversaries, neutrals, and friendly forces, as well as the terrain, weather, and other relevant factors that could impact military operations. When this concept is applied to the information environment, it emphasizes the importance of understanding how information is created, used, manipulated, and perceived by different actors within the battlespace.
- IEBA involves:
  1. **Situational Awareness:** Understanding the current state of the information environment, including the flow of information, key influencers, prevailing narratives, and the presence of misinformation or propaganda.
  2. **Threat Assessment:** Identifying potential threats within the information environment, such as disinformation campaigns, cyber-attacks on information systems, or efforts to undermine trust in institutions.
  3. **Opportunity Identification:** Recognizing opportunities to influence the information environment in a way that supports operational objectives, such as strategic communication initiatives, psychological operations, or cyber operations.
  4. **Decision Support:** Providing commanders and decision-makers with timely and relevant information about the information environment to support planning and execution of operations.
  5. **Protection and Defense:** Ensuring the integrity and security of friendly information systems and countering adversarial information operations.

IEBA is critical in modern warfare and operations, where the control of information and the ability to influence the perceptions and decisions of various actors can be as important as physical military engagements. It requires a multidisciplinary approach, integrating intelligence, cyber operations, psychological operations, public affairs, and other capabilities.

Information Advantage Modeling

Enemy information advantage

- Comms disrupted
- Can't precisely locate enemy with ISR
- Position, Navigation, and Timing (PNT) unreliable
- Manipulated Information fractures unit morale, political resolve, alliance unity, & domestic support
- Deception alters friendly maneuver
- Cyber attacks degrade weapons systems
- Clandestine operations compromised through biometrics and PAI
- Information altered in transit makes reports unreliable
- Public statements about events lags enemy
- Electromagnetic spectrum unavailable
- Enemy recruits local partisans to conduct irregular warfare
- Manufactured crises in non-combatant population diverts resources

Friendly information advantage

- Reliable C2
- ISR provides accurate Situational Awareness
- Position, Navigation, and Timing (PNT) reliable
- Manipulated Information identified, isolated, countered, or thwarted
- Enemy deception is transparent
- Weapons systems/software secure
- Signature management effective
- Reports verified and reliable
- Public statements are first with the truth
- Electromagnetic spectrum available
- Local actors, allies, and domestic populations support and enable friendly actions
- Non-combatants do not interfere with friendly maneuver

Models trained on real-world Operational Environment

Realistic Conditions for Training Audiences to fight for Information Advantage