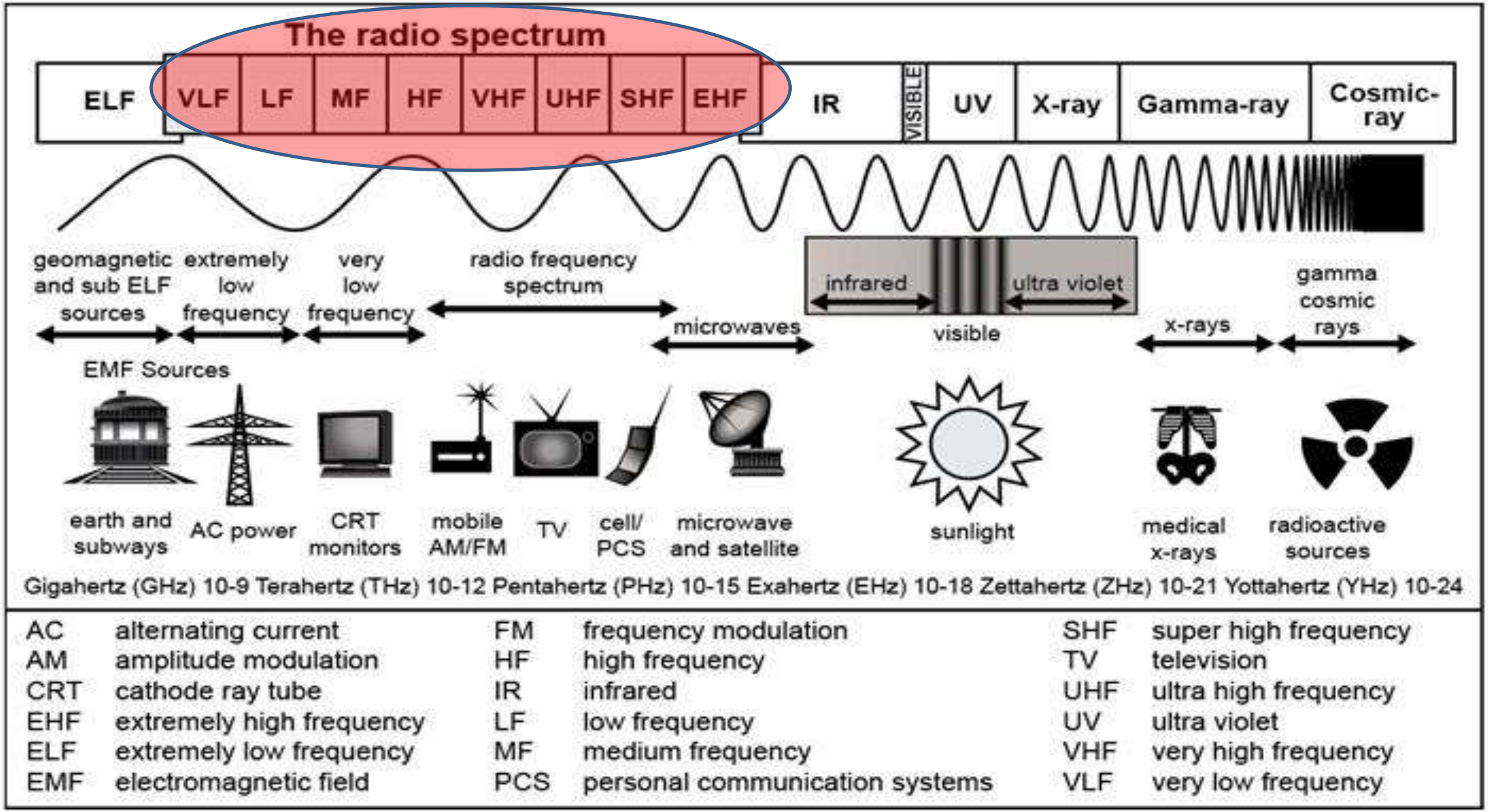
THE CHANGING ROLE OF ELECTRONIC WARFARE

HARNESSING THE POWER OF TECHNOLOGY FOR THE WARFIGHTER . . .

PREVIEW

- HISTORICAL PERSPECTIVE & PRIMER
- WHY THE DELIBERATION ?
- WHERE ARE WE PLACED
- CYBER - EW CONVERGENCE – AI ?
- EW – COGNITIVE DOMAIN ?
- CRYSTAL GAZING & HOW WE NEED TO PROGRESS
- CONCLUSION



AC	alternating current	FM	frequency modulation	SHF	super high frequency
AM	amplitude modulation	HF	high frequency	TV	television
CRT	cathode ray tube	IR	infrared	UHF	ultra high frequency
EHF	extremely high frequency	LF	low frequency	UV	ultra violet
ELF	extremely low frequency	MF	medium frequency	VHF	very high frequency
EMF	electromagnetic field	PCS	personal communication systems	VLF	very low frequency

The Origins of Electronic Warfare

By Wing Commander M. T. THURBON, RAF (Retd)

Men who ignore the past are doomed to relive it.
Santayana

There is a widespread belief that Electronic Warfare (EW) originated early in World War II with the British jamming of the German blind bombing aids Knickebein, X-Gērat and Y-Gērat. In fact what is now called EW has a surprisingly long history and many of the earliest examples of its application still, I believe, hold important lessons for us today. Excellent accounts of the development of electronic warfare in World War II can be found in Alfred Price's books.[1,2] My aim is to retrace the evolution of this subject backwards from 1939.

1919–1939

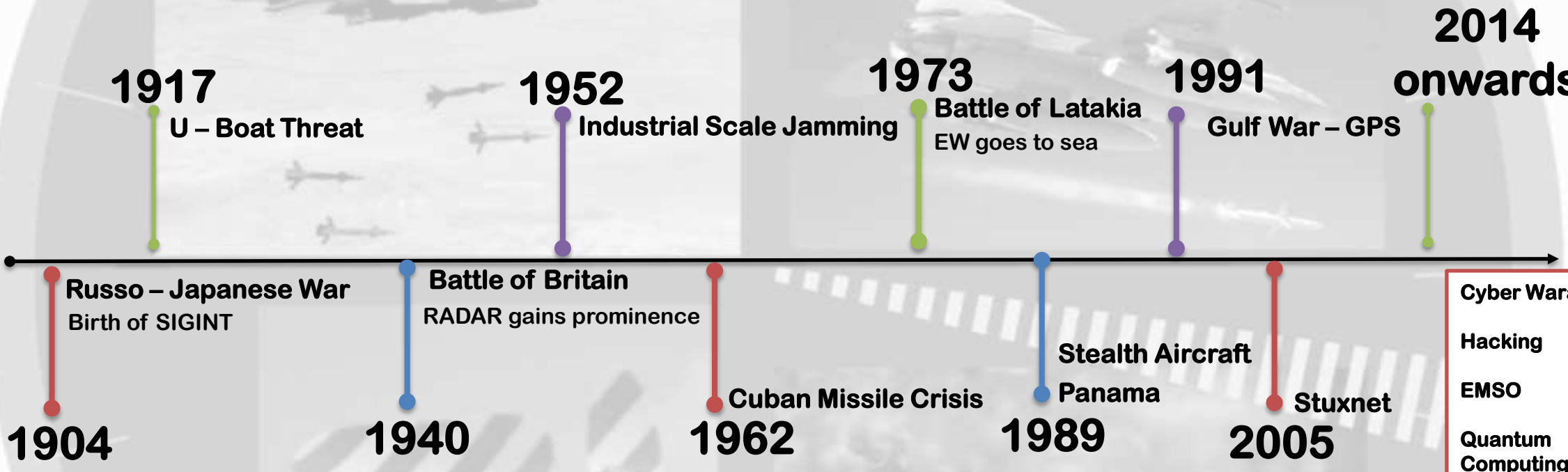
The years between the two world wars saw many conflicts but the scope and nature of most of these precluded the use of EW. Perhaps only in the Spanish Civil War, a proving ground for a wide range of the most modern weapons of the day, were there opportunities for the limited application of counter-measures against communications, although the available references fail to reveal any such operations. This apparent lack of EW activity between 1918 and 1939 does not mean that the subject was completely forgotten. In Great Britain the designers of the early radar systems were, from the very beginning, keenly aware of the possibility of enemy counter-measures. As early as 9 September 1935, less than seven months after the feasibility of radar was first demonstrated, Sir Robert (then Mr) Watson-Watt, in a progress report to the Committee for the Scientific Study of Air Defence, proposed the establishment of what became known as the Chain Home system. His scheme included provision for minimising the effects of interference, especially deliberate jamming. Sir Robert suggested that planning should proceed on the assumption that the anti-jamming design would be effective but he recognised that this hope might be disappointed and that a means of rapidly changing wavelength might have to be provided, although this solution might be expensive. By 1937 the use of multiple wavelengths had become accepted. On 19 October 1935, he was asked by the Committee whether radio-location (as radar was then called) could be defeated by deliberate jamming. In reply Sir Robert defined the conditions that would have to be fulfilled if jamming were to be effective and he discussed the extent to which those conditions might be met by direct jamming from, for example, sites on the Belgian coast. He also considered the possibility of indirect jamming via the ionosphere (these early radars operated in the HF band). He concluded that provided the cover was limited to 0 to 30 degrees in elevation, jamming from ground stations in enemy territory could not defeat the system. It was recognised that airborne jamming could be effective but it was thought that the aircraft could be located by direction finding (DF) and, at least by day, intercepted by fighters. Other suggestions made at the time were for the provision of a reserve and secret frequency for each RDF station and the use of a narrow rotating beam scan. Such was the concern about the vulnerability of RDF to jamming that in 1937 a Jamming Section was set up at Bawdsey to provide various types of jamming to the Anti-Jamming Group and to conduct experiments to assess the effectiveness and probable use of these types of jamming. The work of this section "had the desired result of bringing out many anti-jamming suggestions". In 1938 ground and airborne jammers were used in trials against a number of RDF sites.[3]

ECCM

Work was also in progress elsewhere during this period. An interesting example, because it must be one of the earliest applications of electronic counter-counter measures (ECCM) to a weapon system, occurred in Germany. In 1916 a German, Franz Drexler, had unsuccessfully attempted to convince the authorities of the case for unmanned aircraft controlled by a system of auto-pilot and radio control (the radio control of a model airship had been demonstrated by a German school teacher, Wirth, in 1913). In 1926 the German Army Air Staff was interested in unmanned aircraft for photographic reconnaissance and strategic bombing. Drexler resubmitted his idea and this time to a more receptive audience. Circumventing the terms of the Treaty of Versailles, which prohibited the Germans from operating unmanned aircraft but which said nothing about research, Drexler and a radio expert Max Diekmann, were set to work on the design of a guided missile. Their preferred solution appears to have been a form of command guidance and someone, probably Diekmann, showed a remarkable awareness of the vulnerability of any radio link to jamming. The missile carried a "telemetry" device and signals were transmitted to a control post having two spaced aerial systems with goniometers. The instantaneous position of the vehicle was continuously indicated on a map and the loop must have been closed by a ground transmitter. The problems of protecting the radio signals from jamming had been given much thought throughout and a chain of what were described as selective traps was interposed at both ends.[4] (A wave trap was a circuit placed in series with the aerial of the receiver so as to reject strong interfering signals.) By using a chain of these traps Diekmann ensured that any jammer would

The beginning of EW as a warfare can be traced back to USSR-Japanese War in the year 1905, however, EW came into its own during the Second World War where it was used extensively by the Allies against the German air navigation system used to guide the Luftwaffe in night raids. The well documented campaign wherein EW emerged as a part of warfare was evident in the Tobruk (Africa) Campaign which witnessed interception of radio signals of British Army by the Germans to ascertain the exact location of troop deployment and courses of action. The integrated EW was used for the first time during the Egypt-Israel 1967 Six Day War. The period of the Cold War saw exponential growth in EW technologies. There are numerous instances like Arab-Israel War (1993), Bekka Valley (1982) where the electronic spectrum was used to gain ascendency over the adversary.

HOW THINGS HAVE PROGRESSED



IS SOMETHING MISSING ... ???

WHY THE NEED TO DELIBERATE…..?

Potential Game Changers Through 2035 (The Era of Accelerated Human Progress)

Robotics

40+ countries develop military robots with some level of autonomy. Impact on society, employment.

Vulnerable: Cyber/EM disruption, power systems, ethics without man in the loop.

Formats: Unmanned/Autonomous; ground/air vehicles/subsurface/sea systems. Nano-weapons.

Examples: (Air) Hunter/killer UAV swarms; (Ground) Russian Uran: Recon, ATGMs, SAMs.

Artificial Intelligence

Human-Agent Teaming, i.e., where humans and intelligent systems work together to achieve a physical or mental task. Human and the intelligent system will trade off cognitive and physical loads in a collaborative way.

Weaponized Information enabled by AI that deliberately misrepresents voice and video to influence the political, financial, and military areas.

Internet of Things (IoT)

Trillions of internet linked items create opportunities and vulnerabilities. Explosive growth in low Size Weight and Power (SWaP) connected devices (Internet of Battlefield Things), especially for sensor applications (situational awareness). Greater than 100 devices per human. Significant end-device processing (sensor analytics, sensor to shooter, supply chain management).

Vulnerable: Cyber/EM/Power disruption. Privacy concerns regarding location and tracking.

Sensor to shooter: Accelerate kill chain, data processing and decision making.

Computing

Human computer interaction transformed, processing power increases exponentially.

Interface: From mouse/keyboard/wearables to digital telepathy, centaur systems.

Quantum Computing: From 1&0 binary to quantum superpositions & entanglement (e.g., 0 and 1 at same time).

Big Data: Quantum computing using advanced predictive algorithms/sensing, Internet of Things (IoT) enabled. Must protect against deception.

Sentient Data: Pinpoints who can/cannot access and interact with, without human intervention.

Cyber

Self-configuring, self-protecting computer systems and networks.

Swarms/Semi Autonomous

Massed, coordinated, fast, collaborative, small, stand-off. Overwhelm target systems. Mass or disaggregate.

Electronic Warfare

Radar Jammers: Sophisticated noise or repeaters.

Convergence of RF+Cyber through software defined radios. Controlled modulation can make signals look like noise to interceptors.

ELECTRONIC WARFARE

Potential Game Changers Through 2050 (The Era of Contested Equality)

Convergence – The intersection or merging of many new and potentially revolutionary technologies will create exponential change in the operational environment.

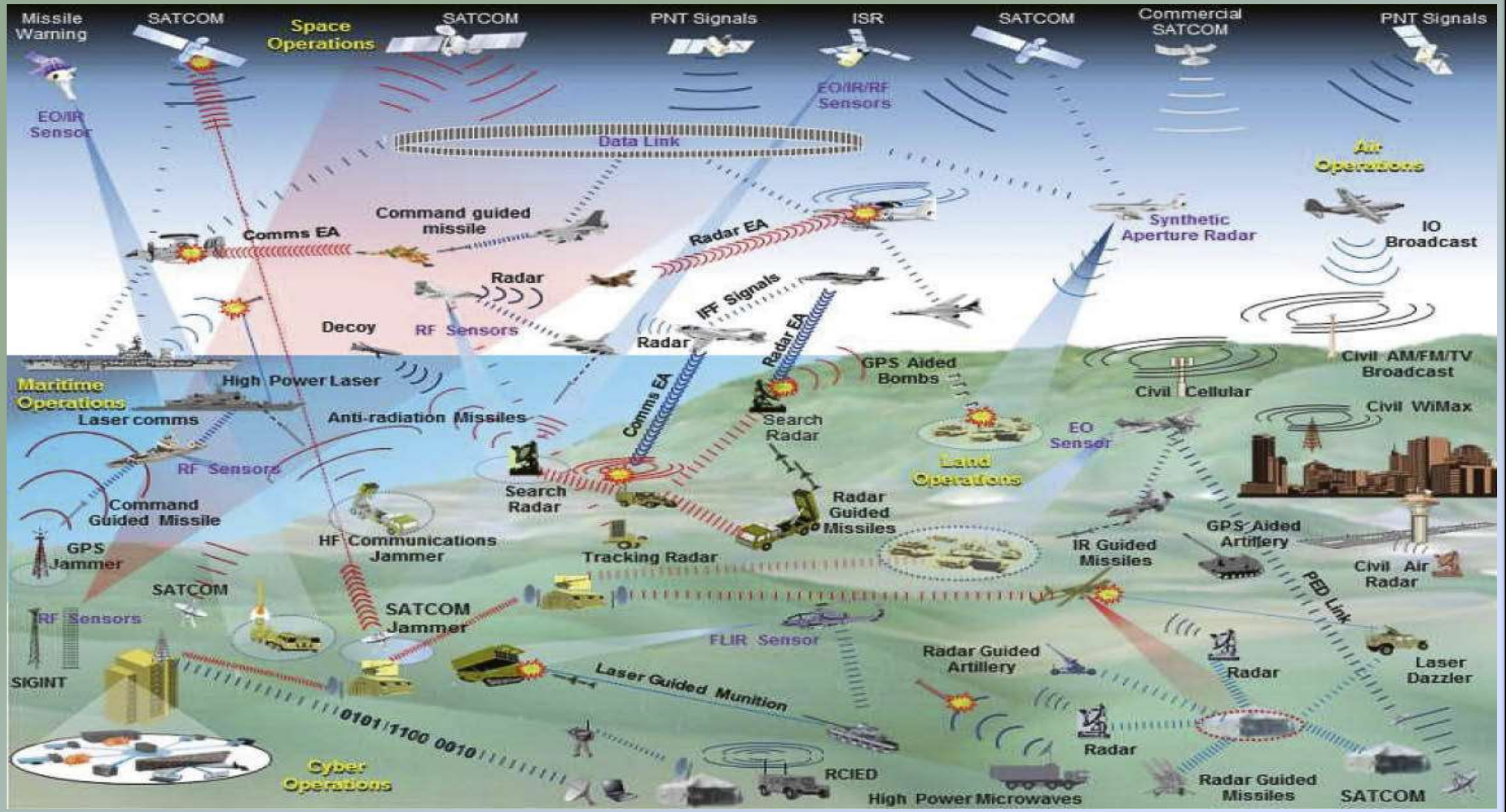
Hyper Velocity Weapons
Rail Guns (Electrodynamic Kinetic Energy Weapons)
Electromagnetic projectile launchers: High velocity/energy and space (**Mach 5** or higher). Not powered by explosive.
No Propellant: Easier to store and handle. **Lower Cost Projectiles**: Potentially. Extreme G-force requires sturdy payloads.
Limiting factors: Power. Significant IR signature. Materials science.
Hyper Glide Vehicles: Less susceptible to anti ballistic missile

Power
Critical driver of future capabilities
Storage/production increa
smaller/lighter.
Strategi ption,
s: Store exponentially
recharge faster.
Renewable Energy: Combining two or more renewable energy sources.
Wireless: Power and charging over the air (long distances).
Nuclear: Very small reactors for the electrified force: small modular advanced nuclear power via DE and electric transportation.

Synthetic Biology
Engineering / modification of biological entities.
Increased Crop Yield: Potential to reduce food scarcity.
Weaponization: Potential for micro-targeting, seek & destroy microbes that can target DNA. Potentially accessible to super-empowered individuals.
Medical Advances: Enhance Soldier survivability.
Genetic Modification: Disease resistant, potentially designer babies and super athletes/Soldiers. Synthetic DNA stores digital data. Data can be used for micro-targeting.
CRISPR: Genome editing.

ELECTRONIC WARFARE
technology. Power
ently problematic.
Po Tunable, lethal, and non-lethal.
Laser: Directed energy damages intended target. Targets: Counter Aircraft, UAS, Missiles, Projectiles, Sensors, Swarms. Must dwell on target.
RF: Attack targets across the frequency spectrum.
Targets: Not just RF: Microwave weapons "cook targets," people, electronics.

Energetics
Defines the relationships of the flow and storage of energy.
LENR: Low Energy Nuclear Reactions
Insensitive Munitions: Chemically stable munitions withstand shock, fire, projectiles; yet explode as intended.
Nano Materials: Miniaturized power sources; reduce bulk, increase yield.



ELECTRONIC WARFARE

Based on MoD Annual report 2018-19

WHERE ARE WE PLACED

BEL-INDIA

रक्षा अनुसंधान एवं विकास संगठन
रक्षा मंत्रालय, भारत सरकार
DEFENCE RESEARCH & DEVELOPMENT ORGANISATION
Ministry of Defence, Government of India

Critical Sub-systems for Integrated EW System 'Samyukta' (SAMISHTI): The first integrated indigenous EW programme 'Samyukta' was successfully designed, developed and commissioned by DRDO in the Indian Army in 2008. DRDO has recently taken a new project for upgradation of critical sub-systems for COM segment of 'Samyukta' and establishment of reference COM entity work posts (HF, VUHF, SALPJ& RDF). During the

EW Systems 'Samudrika' for Capital Ships, Aircrafts and Helicopters for Indian Navy: DRDO has taken up the development of a family of seven EW systems which includes three ship-borne systems (Shakti, Nayan&Tushar) and four air-borne systems (Sarvadhari, Sarang, Sarakshi & Nikash). During August, 2018,

Ground based High Power Microwave (HPM) Directed Energy Weapon System: DRDO has taken up a project to develop a HPM system of RF power in S-band which will be affecting drones at the distance of 5 km. During

Verify Organize Maintain Analyze (VYOMA): DRDO has taken a project to build an easy to use information repository of 'Signal Intelligence Reports' and 'Signal Intelligence Summaries' with semantic querying facilities, social network analysis, spatial and temporal visualization over digital maps. VYOMA Build 1.0 has been deployed at User premises and User training conducted for 22 personnel at Delhi.

Project HIMRAJ for Indian Air Force: The role of the system is to intercept, monitor, analyse and locate adversary's radar transmission in 70 MHz to 40 GHz band. DRDO is responsible for the system design, development of critical sub-system, and realisation of a truncated reference version of the engineered system for Ground Base Mobile ELINT System (GBMES), which are being pursued towards production at BEL.

ELECTRONIC WARFARE

EW DEVP – LEADING NATIONS

This is an advt in the US Navy & Marine Corps website inviting white papers in the yr 2010.

Tech – Thought Process

Unattended ES Systems.

EW Mgt Systems.

Adaptive Sig Processing.

a. Unconventional coordinated ES techniques that cooperatively increase situational awareness across a distributed battlespace;

b. Network-enabled coherent ES methods;

c. Data-link requirements and methodologies for distributed ES systems; and

d. Efficient information management of distributed ES systems.

2. Components and Architectures for Small, Unmanned/Unattended ES Systems

A distributed ES capability will require the development of components and architectures that will support a spatially dispersed array of ES systems, many of which will be on unmanned vehicles or in unattended locations. The objective is to provide broader area coverage for naval (Navy and Marine Corps) EW operations while increasing operational flexibility and combat efficiency and decreasing warfighter workload. Potential areas of investigation include:

a. Low cost ES receivers, particularly with highly-integrated and chip-scale components and sub-systems;

b. Wideband apertures that combine compact size with high gain for ES applications (the ability to share these apertures with EA systems to allow for multiple simultaneous receive/transmit beams is also of great interest);

c. Improving isolation between emitting and receiving apertures on small platforms;

d. Reducing size, weight, and power (SWAP) of ES components and sub-systems;

e. Common signal processing protocols and database techniques that support seamless information exchange between platforms; and

f. Electronic Warfare Battle Management (EWBM) and control of a distributed EW System of Systems (SoS).

3. ES Adaptive Signal Processing

The objective is to improve the capability of naval (Navy and Marine Corps) ES systems in detecting and processing signals in a complex EM environment. Specific challenges to achieving this objective include the increasing density and diversity of signals that span broad frequency bands of the EMS. Potential areas of investigation include:

a. Deinterleaving (i.e., isolating and associating signals from a single emitter in a complex signal environment containing two or more emitters) arbitrary waveforms;

b. Detecting and identifying weak signals of interest (SOI) in the presence of strong interfering signals with similar characteristics (frequency, modulation);

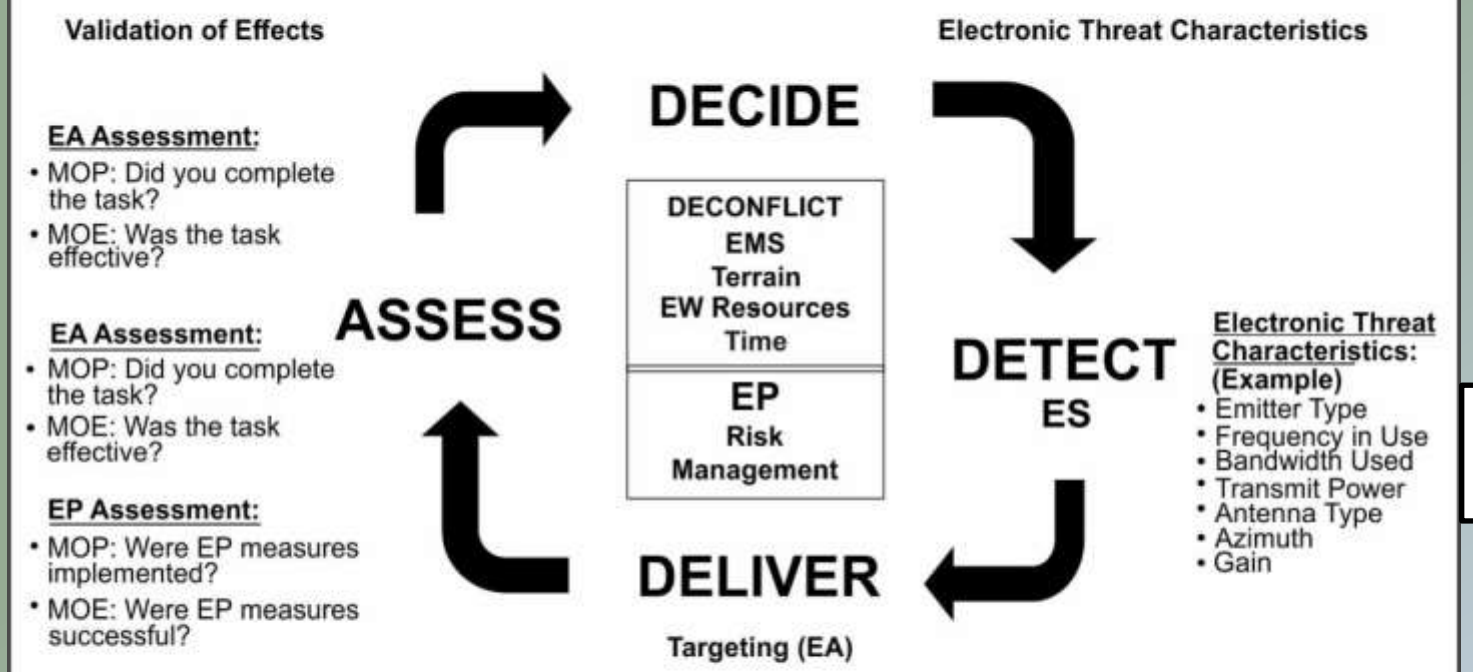
c. Extracting signal parameter to uniquely identify emitters with arbitrary waveforms;

d. Unconventional methods for passively locating, geo-locating, or precisely determining range to signal emitters, particularly from a single ES platform/sensor; and

G-6 (S-6)
- Spectrum Management
- Frequency Deconfliction
- JRFL

CEMA SECTION
- DDR's Internet and Endstate
- EW Task and Purpose
- EW Trigger/Times
- EW Targets (Location,
- Characteristics
- EW PACE Plan

G-2 (S-2)
- IPB, OPE,
- HVTL, HPTL
- Enemy COA
- Enemy COA



LEGEND

CEMA	cyber electromagnetic activities
COA	course of action
DDR	disarmament, demobilization and reintegration
EA	electronic attack
EMS	electromagnetic spectrum
EP	electronic protect
ES	electronic warfare support
EW	electronic warfare
G-2	assistant chief of staff, intelligence
G-6	assistant chief of staff, signal
HPTL	high payoff target list
HVTL	high value target list
IPB	intelligence preparation of the battle field
JRFL	joint restricted frequency list
MOE	measures of effectiveness
MOP	measures of performance
OPE	operational preparation of the environment
PACE	primary alternate contingency emergency
S-2	intelligence staff officer
S-6	signal staff officer

ADAPTED FROM ATP 3-12.3 US ARMY PUBLISHED IN JULY 2019

The EW Cycle Targeting Process –Process Flow

Asymmetric Warfare Group

RUSSIAN NEW GENERATION WARFARE HANDBOOK



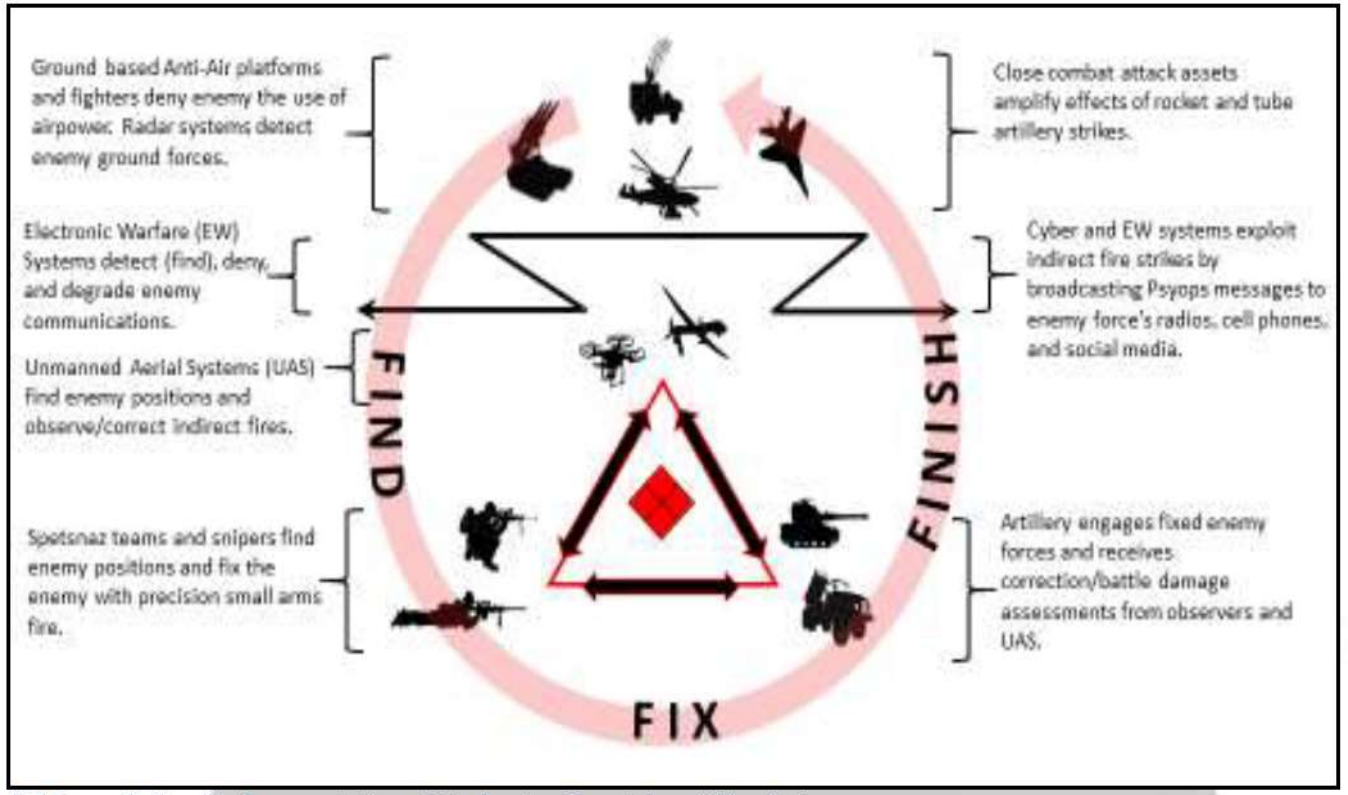




Version 1: December 2016

A handbook for U.S. Army formations to increase awareness of Russian tactics, near-peer capabilities, and current U.S. non-material solutions to mitigate the threat posed by Russian proxies.

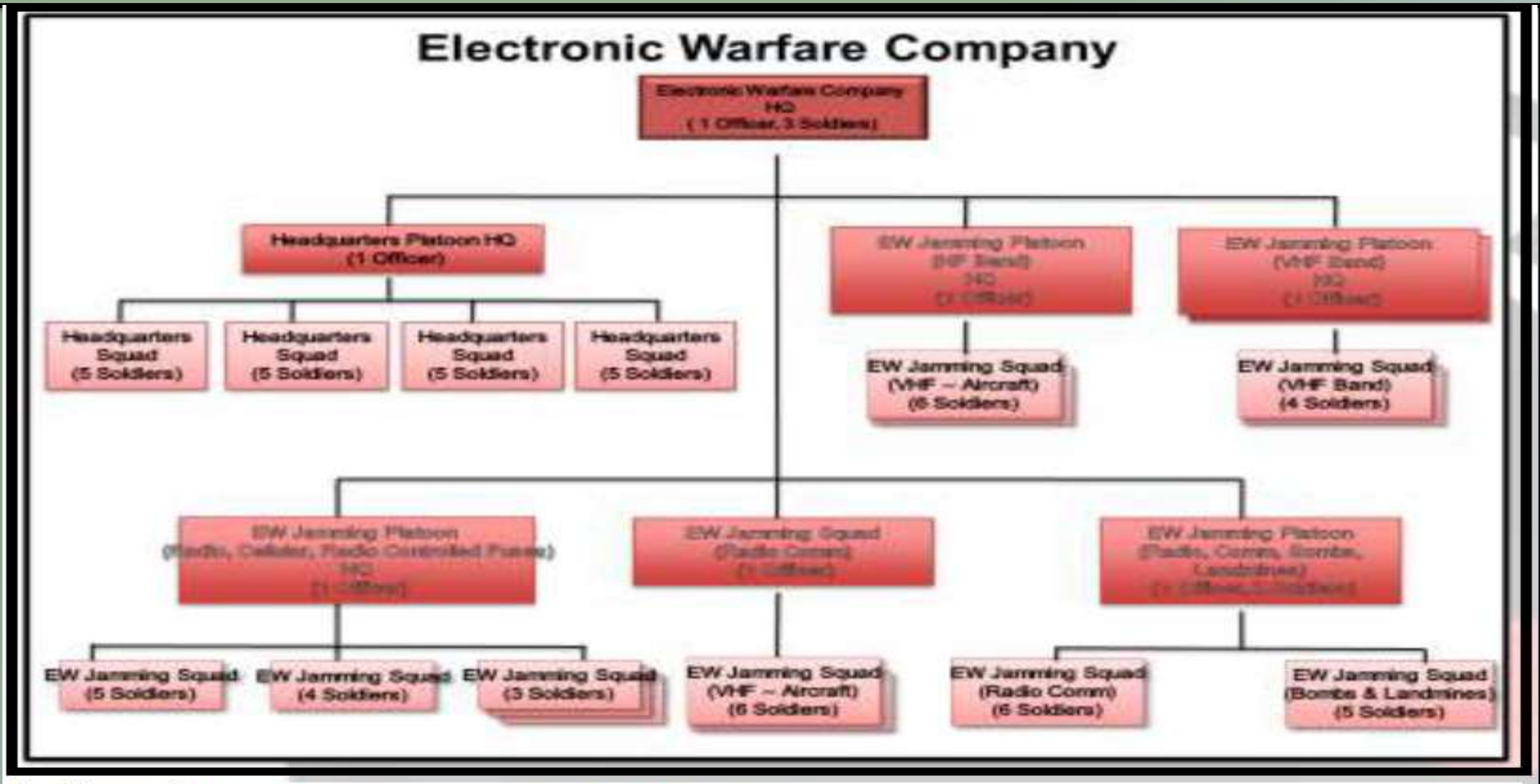
(U) An overarching layer of electronic warfare systems protects this target acquisition cycle. These EW platforms can collect electromagnetic signals and determine their location, thereby providing



(U) Figure 8: Graphic Representation of the Russian Target Acquisition Cycle

(U//FOUO) Cyber vs EW

(U//FOUO) Cyber is an emerging capability for combat commanders and currently come with added restrictions due to the nature of that capability. Commanders should be aware that similar effects can be achieved with EW as with cyber if properly articulated during the planning and orders production process. Commanders should become familiar with these concepts and plan with respect to their *effects* in the battle space instead of what *assets* are used.



(U//FOUO) Figure 12: Electronic Warfare Company

(U//FOUO) As important as the capability to operate in an electr environment, is the ability to recognize that enemy forces are causing the jamming first reaction of soldiers and leaders is to blame faulty equipment, or a b spend time trying to trouble-shoot and fix problems that are actu more dangerous, is the Russian ability to insert false readings a Command System (MCS). Imagine the danger of a commande units. Significant dangers exists from a commander's sole re using that information to enforce fire control measures.

(U//FOUO) The Russian Armed Forces have de component units) based entirely on their electronic capability to jam or spoof GPS signals. GPS units, to electronic warfare systems that can either co

For Russia, the conflict in Syria is about more than just keeping the Bashar al-Assad regime in power. It has also provided a testing ground for Russian weapon systems, including jets, cruise missiles, and according to Israeli sources, new cyber and GPS-jamming techniques.

One of the clear advantages gained by the Russians in Syria is the ability to test their cyber defence and offensive tools against the best Western defence technologies, including the Israeli Air Force's F-35, Arrow anti-ballistic missile defence systems and highly classified unmanned aerial systems.

Israel too is a cyber power. Apart from numerous private companies developing offensive and defensive cyber tools, the Israeli Defence Force's (IDF) 8200 intelligence Corps unit is responsible for collecting signal intelligence (SIGINT) and code decryption. Military publications refer to this unit as the Central Collection Unit of the Israeli Intelligence Corps. It is also sometimes called the Israeli SIGINT National Unit (ISNU). This unit, alongside others, are responsible for defending Israeli weapon systems from cyber attacks and allowing the most advanced weapon systems to operat in GPS-denied environments.

Soldiers must be proficient in map reading and land navigation his threat. Additionally, advances in Russian military capabilities discover a unit's location based on their electronic signatures (such as etc.) and engage friendly forces with effective fires based on that

step to mitigating the threat posed by Russian EW capabilities is to Cyber and general electronic footprint. Commanders and NCOs need to take ce on electronics and begin to formulate small unit-level SOPs. Recently the adre of cyber advisers designed to provide just this input at the tactical level. heavy demand, having a cyber-adviser can greatly benefit a command by assisting ing what equipment might be more or less vulnerable to enemy EW attack. Once this s been created, leaders will be able to see what communications nodes could come nd develop ways to communicate and operate without over-reliance on critical nodes.

ELECTRONIC WARFARE

The Chinese have adopted a formal IW strategy called “Integrated Network Electronic Warfare” (INEW) that consolidates the offensive mission for both Computer Network Attack (CNA) and Electronic Warfare (EW).

The PLA's doctrine for fighting Local Wars Under Informationzed Conditions, the current doctrine that seeks to develop a fully networked architecture capable of coordinating military operations on land, in air, at sea, in space and across the electromagnetic spectrum.

The 3rd Department maintains an extensive system of signals collection stations throughout China with collection and processing stations co-located with each of the PLA's Military Region Headquarters.

GSD 4th Department, also referred to as the Electronic Countermeasures Department (ECM), oversees both operational ECM units and R&D institutes conducting research on a variety of offensive IW technologies.

ORF OCCASIONAL PAPER

203

JULY 2019

Electronic and Cyber Warfare: A Comparative Analysis of the PLA and the Indian Army

KARTIK BOMMAKANTI

In 1999, PLA Major General Dai Qingmin was the key advocate behind the adoption of China's integrated view of CW and EW operations as part of the PLA's Information Warfare (IW) strategy. Dai secured a promotion to head the erstwhile 4th Department of the Chinese General Armaments Department (GAD). He made the case for fusing EW with Computer Network Operations (CNO). He defined Information Operations (IO) as a series of operations with information systems as the direct operational target, and with electronic warfare and a computer network war as the principal form."[42]

According to the PLA, EW and CW are not mutually exclusive; it is necessary to recognise their convergence and integration to dominate information operations during wartime. Dai Qingmin called it Integrated Network Electronic Warfare (INEW) composed of the "...organic combination of electronic warfare and computer network warfare." As

ELECTRONIC WARFARE

WHAT DO WE INFER ?

DO WE SEE SOME KIND OF CONVERGENCE ?

INTEGRATION OF VARIOUS THEMES ??

United States Government Accountability Office

GAO

Report to Congressional Committees

EW ADAPTATION

August 2019

Why GAO Did This Study

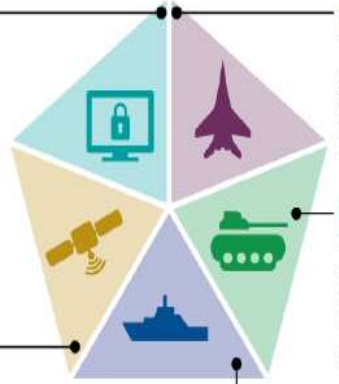
The rise of great-power competitors, such as China and Russia, prompted the Army to transform the way it plans to fight. The Army is developing a new warfighting concept to guide how its forces will engage jointly with other services in multiple domains, especially in cyber and space.

The House Armed Services Committee included a provision in House Report 115-200 accompanying a bill for the National Defense Authorization Act for Fiscal Year 2018 for GAO to review the Army's implementation of the concept. Among its objectives, this report addresses (1) how the Army is changing its doctrine, organizations, and training in order to execute multi-domain operations; and (2) the extent to which the Army has established new cyber and electronic warfare units, including any challenges faced by these units, and whether the Army assessed risks associated with its plan to establish these units.

The Five Warfighting Domains Envisioned by the Army Operating Concept

Cyber
A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Space
The area above the altitude where atmospheric effects on airborne objects become negligible.



Air
The atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible.

Land
The area of the Earth's surface ending at the high-water mark and overlapping with the sea domain in the landward segment of the shoreline.

Sea
The oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the areas adjacent to the shoreline.

What GAO Recommends

GAO is making three recommendations, including that the Army comprehensively assess the risk of staffing, equipping, and training the cyber and electronic warfare units that it has activated at an accelerated pace, and to do so for new organizations it plans to activate in an accelerated manner for multi-domain operations. The Army concurred with one recommendation and partially concurred with two recommendations. GAO clarified the recommendations, as discussed in the report.

RUSSIA – NEW STRATEGIC DOCUMENT

- STATE CONT OVER DEVP OF EW CAPB
- INTEGRATE MIL EW DOMAIN WITH OTHER STATE ACTORS
- EXPLOIT R & D
- FURTHER DEVP OF EW EDUCATIONAL & RESEARCH SYS
- EXPAND MIL TECH COOPERATION

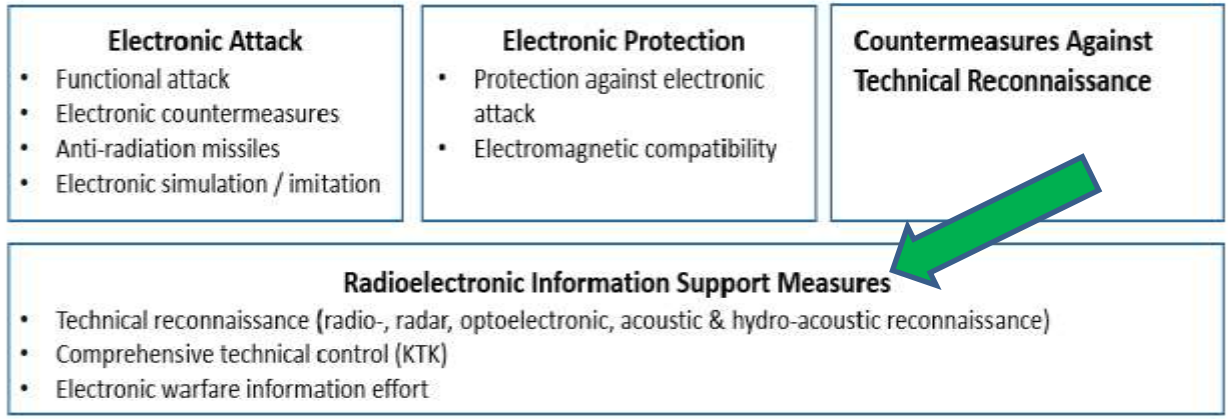


Figure 1: The modern Russian EW definition with its four subdivisions.
Source: Guzenko & Moraresku (2017).

In 2013 the five main directions of the then newly adopted strategy document were revealed by the former commander of the EW Troops. These are: first, improving state control over the functioning and development of EW; second, integrating the military EW domain with other state domains significant for national security; third, exploiting accomplishments in R&D in order to procure a new generation of EW systems; fourth, further development of the EW educational and scientific research system; and, fifth, expanding military-technical cooperation and increasing the export potential of EW systems (Doskalov 2013).

OUTCOMES

- CONVERGENCE OF DOMAINS – CYBER & EW FUSION
- SPECTRUM & EW PLG / MGT AS A MAJ PLAYER
- COGNITIVE EW
- ROLE OF AI
- WAY AHEAD – AS A FUSION OF TECHNOLOGIES

EW-CYBER RELATIONSHIP

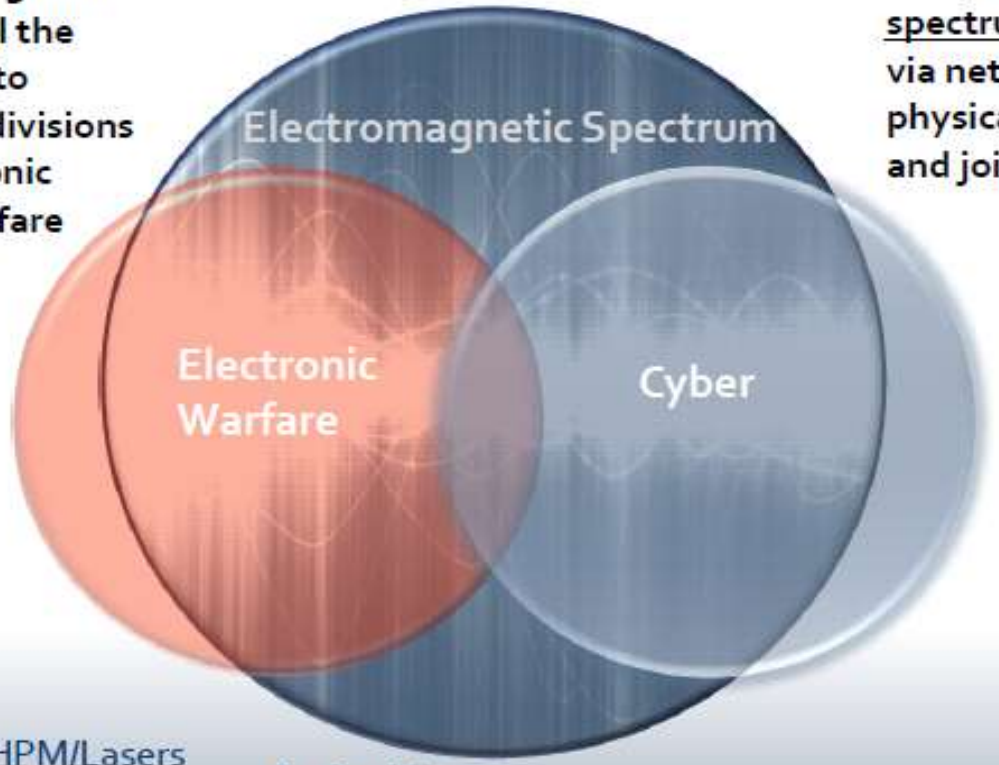
- **Electronic Warfare** - military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the adversary
- **Cyber Warfare** involves crippling adversaries through information systems and the Internet
- Electronic warfare and cyberspace operations are complementary and have potentially synergistic effects
  - Example: Use EA system to deliver malicious code into cyberspace via a wireless connection - "EW - delivered computer network attack"
- The convergence of EW and Cyber brings with it new opportunities and challenges
- Modern networked systems (EW and threat) bring additional capabilities to the table, but are vulnerable to cyber-attack, because they are predominantly software defined
- We have to use the EMS **and** Cyber in order to monitor and achieve the desired military effects on the modern battlefield

SOURCE WEBSITE: ASSOCIATION OF OLD CROWS

EW-to-Cyber Relationship

EW: Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Major subdivisions are: Electronic attack, Electronic Protection and Electronic warfare support

Cyber: Joint Pub 3-12: A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures. This includes BLOS/C2 and joint and coalition airborne networks



EW Capabilities:
- SIGINT
- C3CM
- SEAD
- Chaff/Flares/Decoys
- Directed Energy Wpsn, HPM/Lasers
- Kill Chain Effects:
  < 2minutes

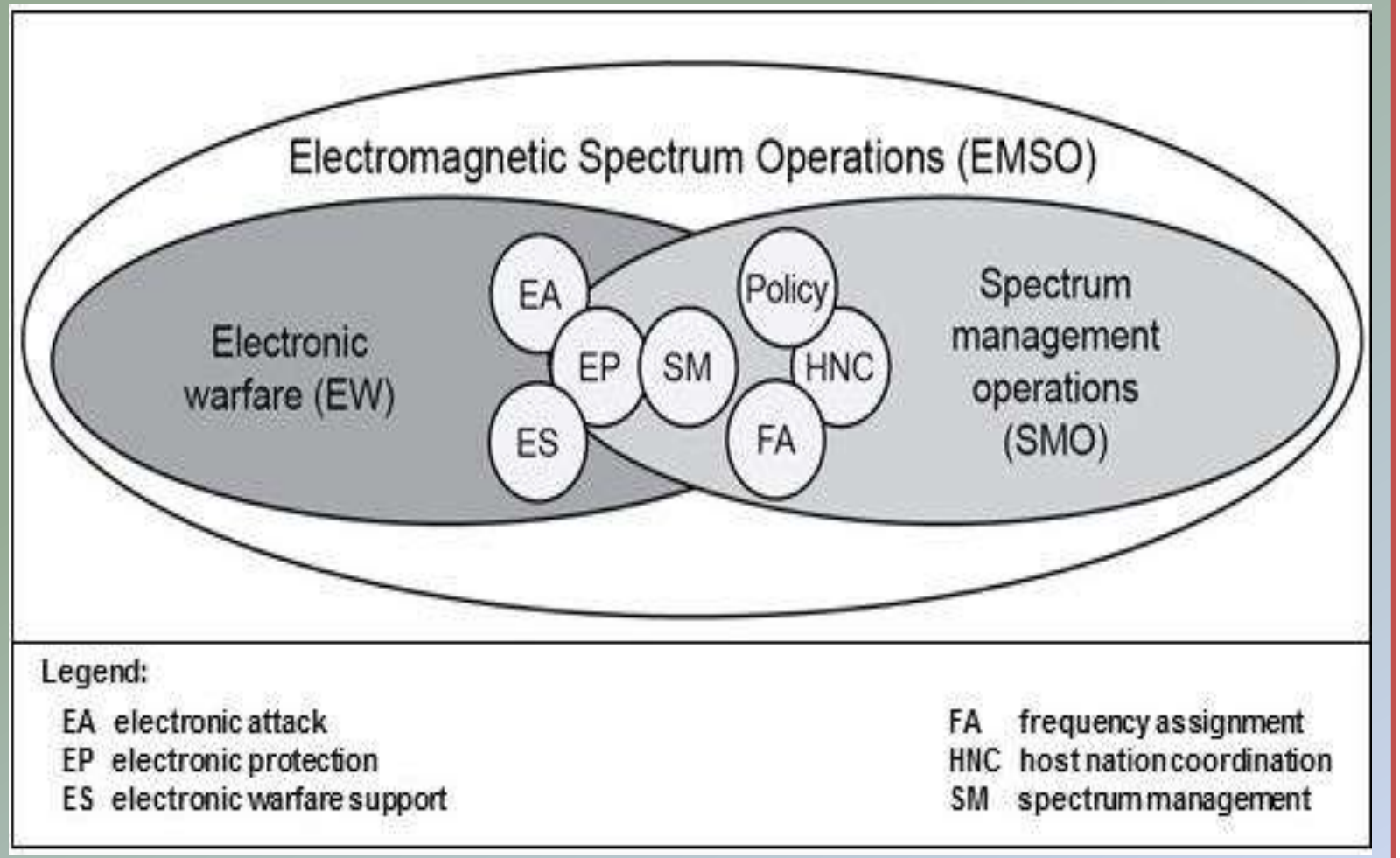
Authorities:
- Title 10: US Military Forces (Overt)
- Title 50: Intelligence Agencies (Covert)
- Title 18: Justice Agencies (Crime)

Cyber Capabilities:
- Computer Network Attack
- Computer Network Defense
- Computer Network Exploit
- Malware, Transnational Threats
  Credit card/Identity Theft
- Kill Chain Effects:
  < 300 microsecs

USES OF EW – CYBER CONVERGENCE

- THE FIRST-STRIKE ADVANTAGE OF CYBER WEAPONS COMPARED TO NUCLEAR WEAPONS IS VASTLY DIFFERENT AND RESULTS IN A FIRST-STRIKE STRATAGEM USING CYBER WEAPONS FOR DETERRENCE AS NOT USEFUL.
- A FIRST-STRIKE ADVANTAGE IS GAINED WHEN COUNTERING CYBER WEAPONS AND SOME CONVENTIONAL WEAPONS.
- FIRST-STRIKE IN CYBERSPACE IS LIKELY TO BE THE MOST USEFUL FOR COERCION BY DENIAL, LESS USEFUL FOR COERCION VIA RISK, AND LEAST USEFUL FOR COERCION THROUGH PUNISHMENT.
- A FIRST-STRIKE STRATAGEM FITS VERY WELL WITH STRATEGIC AND MILITARY AIMS, ALTHOUGH A DECLARATORY STRATAGEM AIMED AT DETERRENCE IS NOT USEFUL IN CYBERSPACE, ONE THAT IS NOT DECLARED COULD BE VERY USEFUL.
- TECHNOLOGY AND CYBERSPACE IS CONTINUOUSLY CHANGING, WHICH WILL AFFECT THE FUTURE USEFULNESS OF A FIRST-STRIKE STRATAGEM FOR DETERRENCE.

SPECTRUM MANAGEMENT

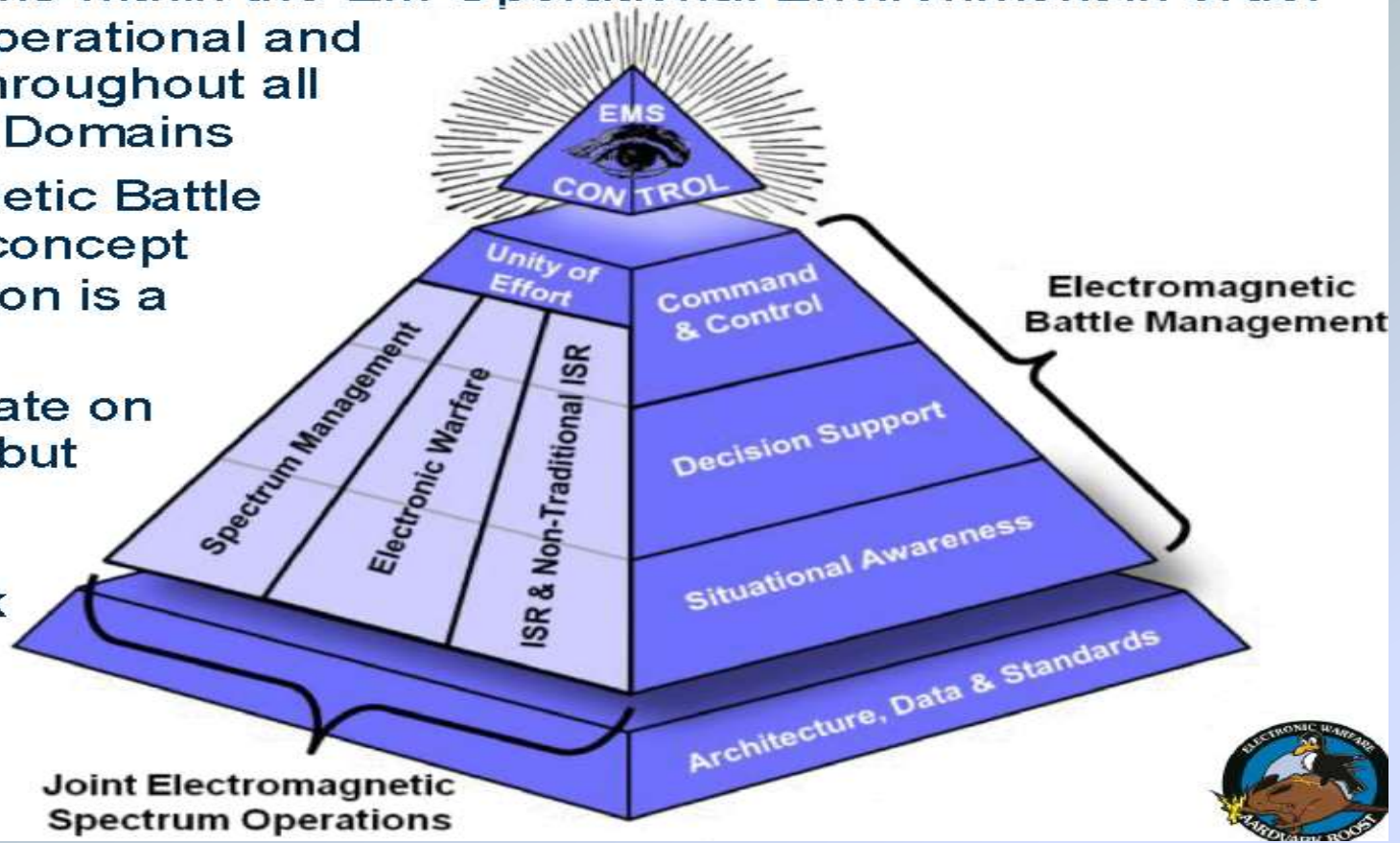


Electronic warfare refers to military action involving the use of electromagnetic and directed energy
to control the electromagnetic spectrum or to attack the enemy

EW capabilities enable Army forces to create conditions and effects in the EMS to support the commander's intent and concept of operations. EW includes EA, EP, and ES and includes activities such as electromagnetic jamming, electromagnetic hardening, and signal detection, respectively. EW affects, supports, enables, protects, and collects on capabilities operating within the EMS, including cyberspace capabilities.

EM BATTLE MANAGEMENT

- Up to recently spectrum management was done through the use of (Joint) Allocated/Restricted Frequency Lists – but this concept has outlived its usefulness
- Requirement - The ability to Dynamically Monitor, Assess, Plan, Integrate and Direct EW operations within the EM Operational Environment in order to achieve Strategic, Operational and Tactical EMS Control throughout all phases of conflict in all Domains
- This is the Electromagnetic Battle Management (EMBM) concept
- EMS data standardization is a requirement
- EW can no longer operate on a 'need to know' basis, but instead on a 'need to securely share' basis
- Biggest stumbling block - people don't want to share their data



4 OCTOBER 2019 NEWS

Raytheon electronic warfare tool for US Army in final development

Raytheon is developing the final phase of the electronic warfare planning and management tool (EWPMT) for the US Army.

The EWPMT tool is designed to assist the army in planning and managing electronic warfare.

It provides the service with the ability to plan, manage and control sensors and systems in the electromagnetic spectrum.

The tool is part of the US Army's Integra
information to operators in a crowded s

EWPMT allows for coordination
the command post.

Under a contract from the US Ar
(CD4), over the next 24 months.

CD4 is the final stage of a fully operatin

"And because it uses open architecture, the tool can be shared with other military services."

The open architecture design of the tool allows it to execute cyber effects in multi-domain operations.

Raytheon already delivered EWPMT CD1 and CD2, and is working on the third Capability Drop.

CD3 enables using the tool in a tactical environment to tackle threats.

In addition, the company incorporated the functionality of Raven Claw, a mobile version of EWPMT, in CD3.

Using Raven Claw, operators can control signals in the field without the need for a host server.

The CD4 contract will include further development of software and the user interface to enable a more connected, mobile system, Raytheon said.

Source: Army Technology.com

RAVEN CLAW

INFORMATION OVERLOAD: VISUALISING ELECTRONIC WARFARE TO MANAGE DATA PROLIFERATION

ELECTRONIC WARFARE

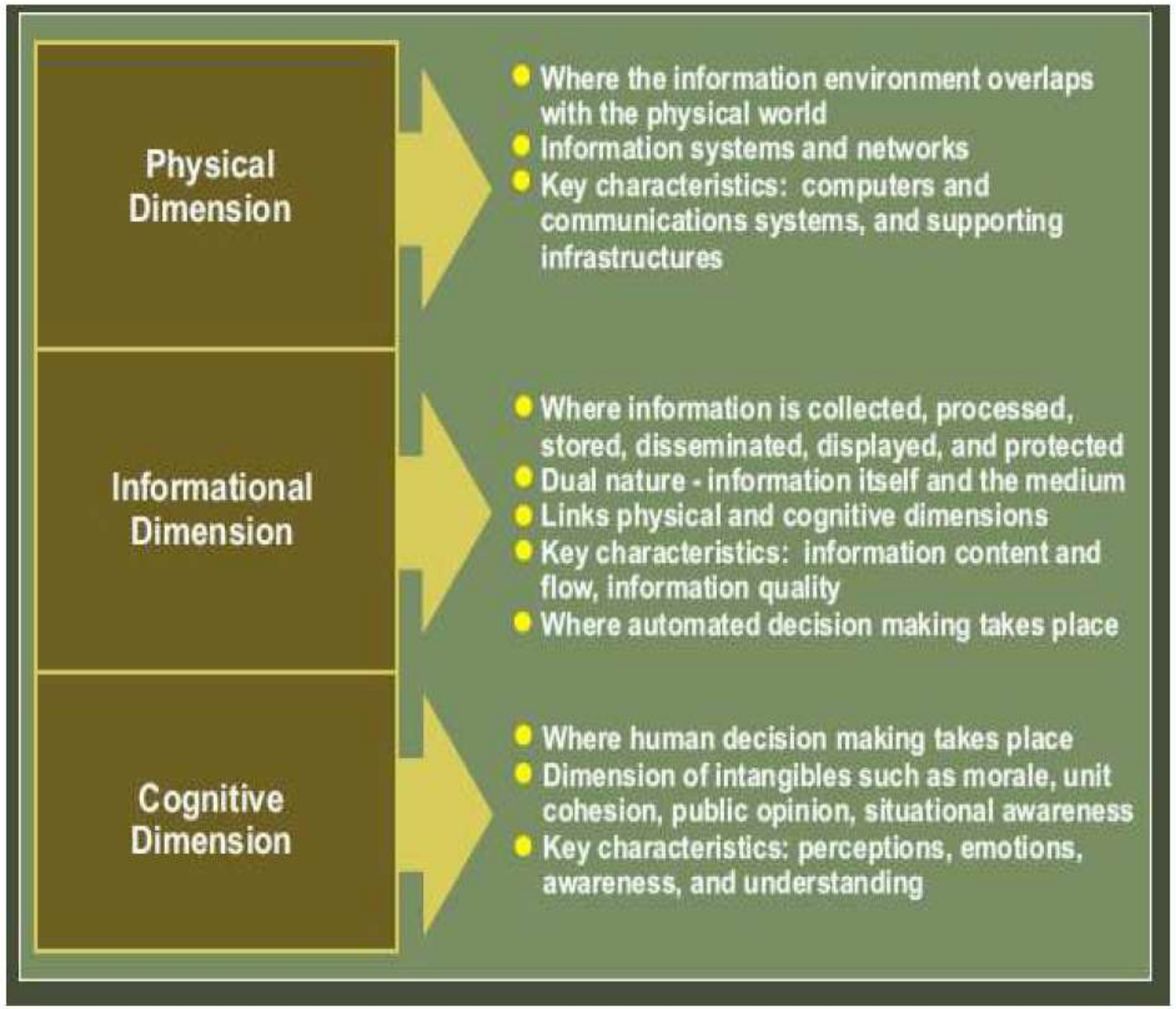
Resilient Synchronized Planning and Assessment for the Contested Environment (RSPACE)

Lt. Col. Jimmy Jones

RSPACE seeks to create a revolutionary distributed planning capability to provide resilient command and control (C2) and to manage complex military operations even when communications are limited and unreliable. RSPACE is developing human-centered software decision aids that, based on the commander's intent, will help operators throughout the C2 enterprise control daily operations in a complex battlespace – composing mission packages (coordinating across the network as needed), responding to emerging opportunities, and assessing progress towards achieving the commander's intent. RSPACE is focused on the operational level of the air operations domain.

Source: DARPA website

COGNITIVE EW



The cognitive dimension includes the mind of the decision maker and the target audience. This is the dimension in which people think, perceive, visualize, and decide. Sometimes — i.e. during psychological operations — it is the most important of the three dimensions. This dimension is also affected by a commander's orders, training, and other personal motivations. Battles and campaigns can be lost in the cognitive dimension. Factors such as leadership, morale, unit cohesion, emotion, state of mind, level of training, experience, situational awareness, as well as public opinion, perceptions, media, public information, and rumors influence this dimension

COGNITIVE EW

COGNITIVE EW- A2F2T2EA4 – AUTONOMOUSLY ANTICIPATE FIND FIX TRACK TARGET ENGAGE & ASSESS ANYTHING ANYTIME ANYWHERE

DIFFERENT FROM SOFTWARE DEFINED – NOT PRE PROGRAMMED. COGNITIVE SYS WILL RECONFIGURE ITSELF ON THE FLY

CURRENT REALITY – RELIANCE ON LIBRARIES OF SIGNATURES/ DATABASE – IF NEW WAVEFORM USED THEN ASSESSMENT CYCLE IS LONG DRAWN – TIME PENALTY

CURRENT REQUIREMENT – OPEN SYSTEM ARCHITECTURE & PLUG & PLAY APPROACH

WHAT IS BLADE

THE BEHAVIORAL LEARNING FOR ADAPTIVE ELECTRONIC WARFARE (BLADE) PROGRAM IS DEVELOPING THE CAPABILITY TO COUNTER NEW AND DYNAMIC WIRELESS COMMUNICATION THREATS IN TACTICAL ENVIRONMENTS.

BLADE IS ENABLING A SHIFT FROM TODAY'S MANUAL-INTENSIVE LAB-BASED COUNTERMEASURE DEVELOPMENT APPROACH TO AN ADAPTIVE, IN-THE-FIELD SYSTEMS APPROACH.

THE PROGRAM WILL ACHIEVE THIS BY DEVELOPING NOVEL-MACHINE LEARNING ALGORITHMS AND TECHNIQUES THAT CAN RAPIDLY DETECT AND CHARACTERIZE NEW RADIO THREATS, DYNAMICALLY SYNTHESIZE NEW COUNTERMEASURES, AND PROVIDE ACCURATE BATTLE DAMAGE ASSESSMENT BASED ON OVER-THE-AIR OBSERVABLE CHANGES IN THE THREAT.

THE CYBER EDGE

ELECTRONIC WARFARE

General Dynamics SignalEye™ solution provides spectrum situational awareness by automating the classification of signals through the use of machine learning. This electronic warfare software provides tactical warfighters and security personnel with a timely, accurate view of the threat in the RF spectrum SignalEye is always on – learning and alerting you to the signals that threaten you and your mission.

DETECT, ISOLATE
AWARENESS

General Dynamics provide warfighters and secu ew of the threat in the RF spectrum an nds in the adversary's behavior. SignalEye doe d hardware acceleration. In a tactical context, this ele are software deploys on a commodity hardware as an add-on to a front end system

Features At A Glance

- Machine Learning – signal classification using convolutional neural networks (CNN)
- Data Driven – detection capabilities based on neural network training
- Streaming – signal detection in streaming digital RF data
- Software Only – solution runs on general purpose computer
- Hardware Independent – RF front-end agnostic
- Mission Independent – integrates with existing user-focused mission interfaces
- Standards Based – supports VITA-49, VITA Radio Transport
- Public API – C/C++, Python, Java, Scala

COGNITIVE AI

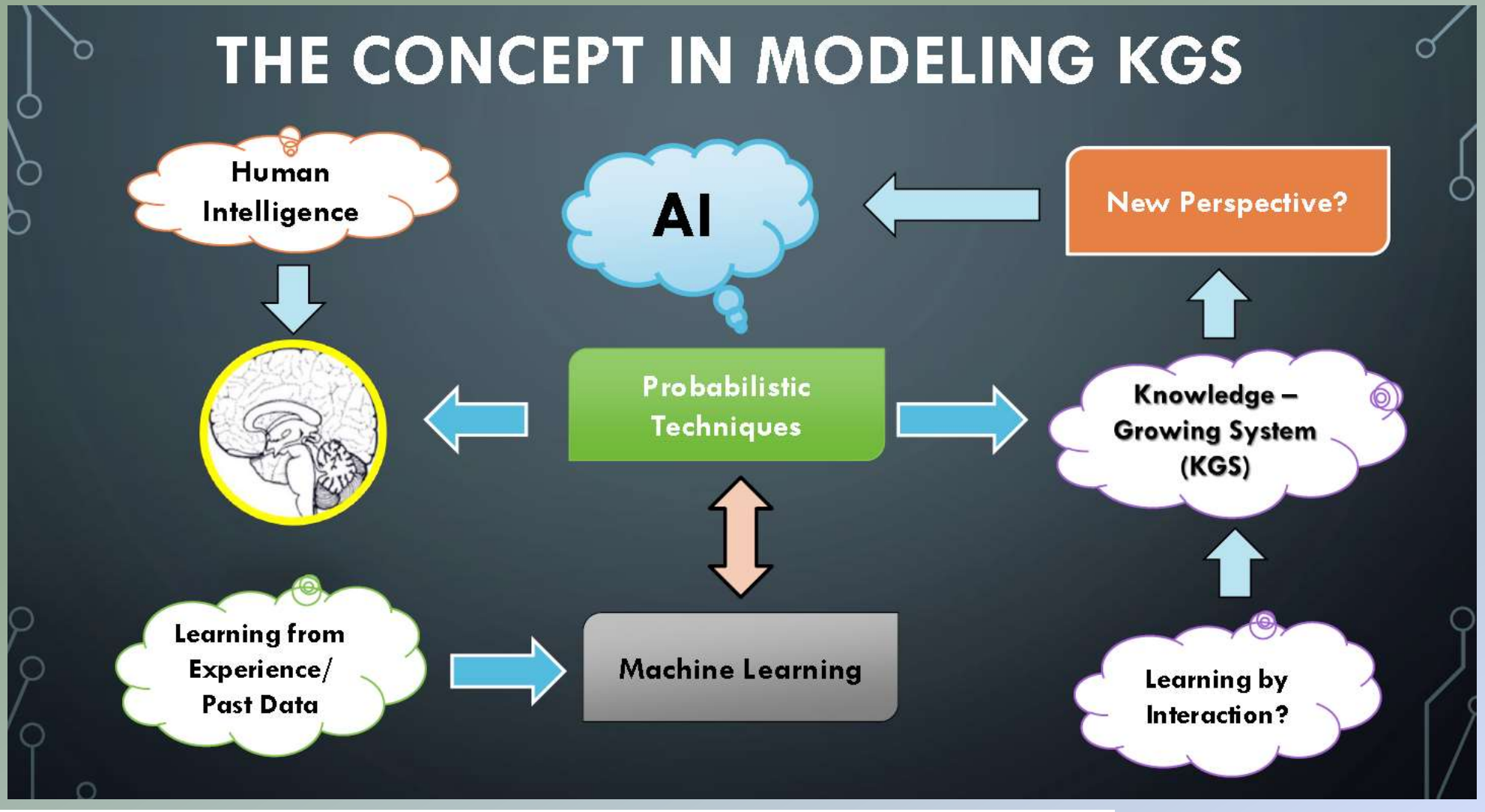
Cognitive Artificial Intelligence

Artificial Intelligence which applies **Cognitive approach** in building systems that are able to **grow its own knowledge by making interaction** with the environment

(Arwin Datumaya Wahyudi Sumari & Adang Suwandi Ahmad, 2017)

CONCLUDING REMARKS

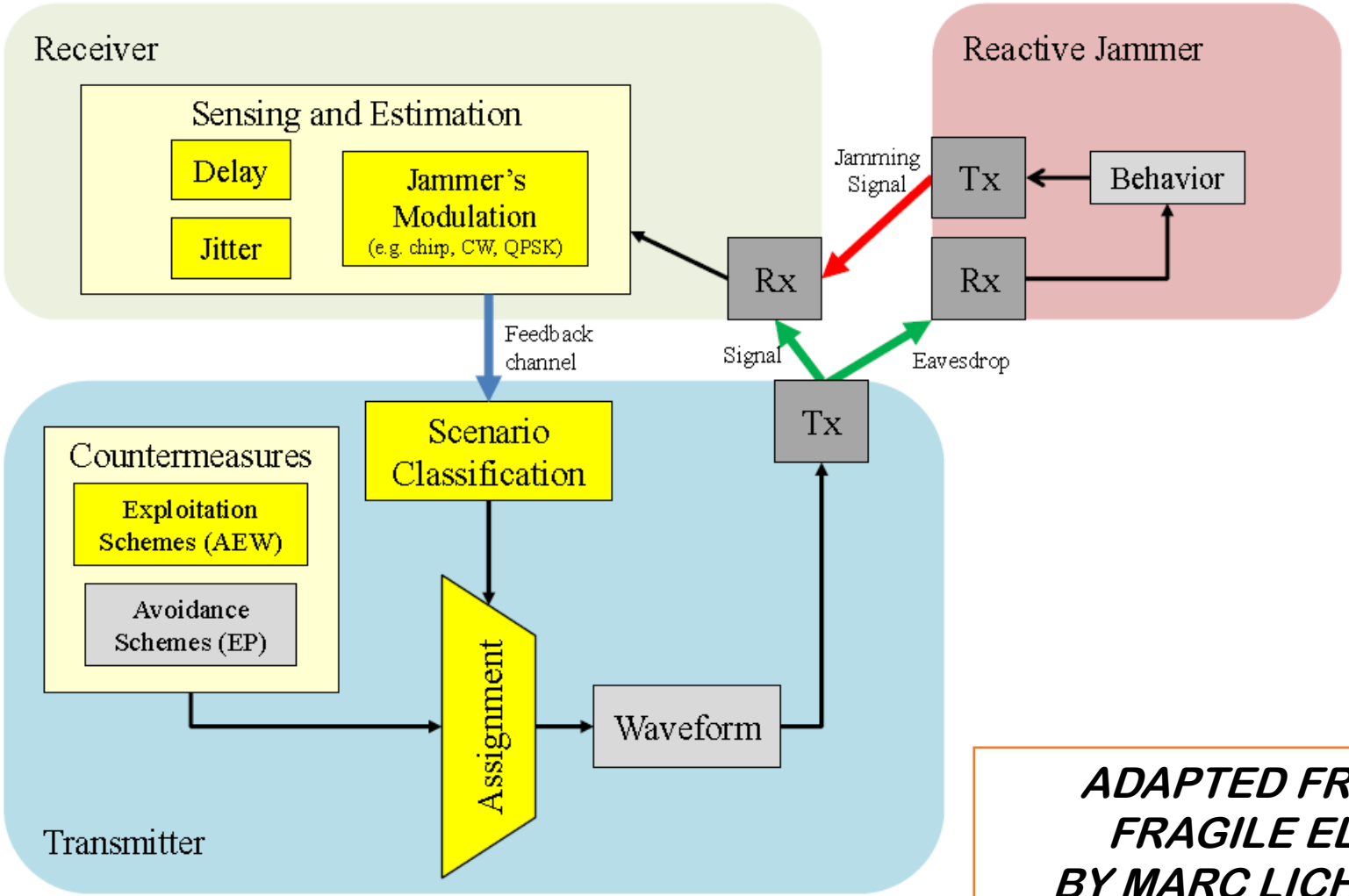
- Cognitive Artificial Intelligence is **a new perspective in AI which emulates the way of human thinks that is approached from Cognitive perspective**
- KGS as the foundation of CAI is **able to show the ability to learn by interaction with the environment directly**, which successfully implements Contructivism theory
- KGS is able to generate/grow the knowledge even with **small number of data and needs no training as other methods in AI**
- KGS **needs more applications** to ensure its robustness



COGNITIVE ARTIFICIAL INTELLIGENCE: A NEW PERSPECTIVE IN ARTIFICIAL INTELLIGENCE

Arwin Datumaya Wahyudi Sumari
Indonesian Air Force Headquarters

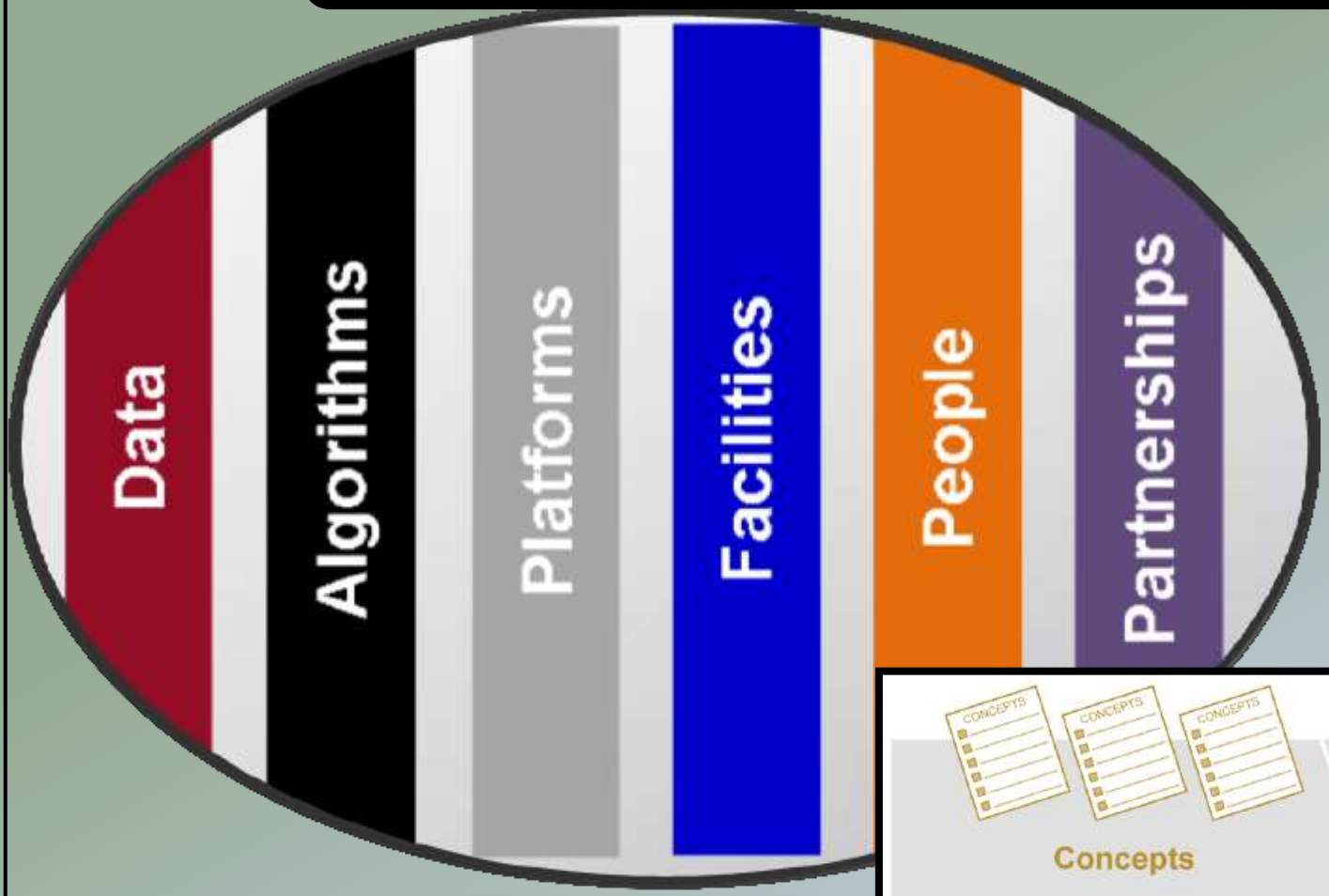
ANTI - FRAGILE EW

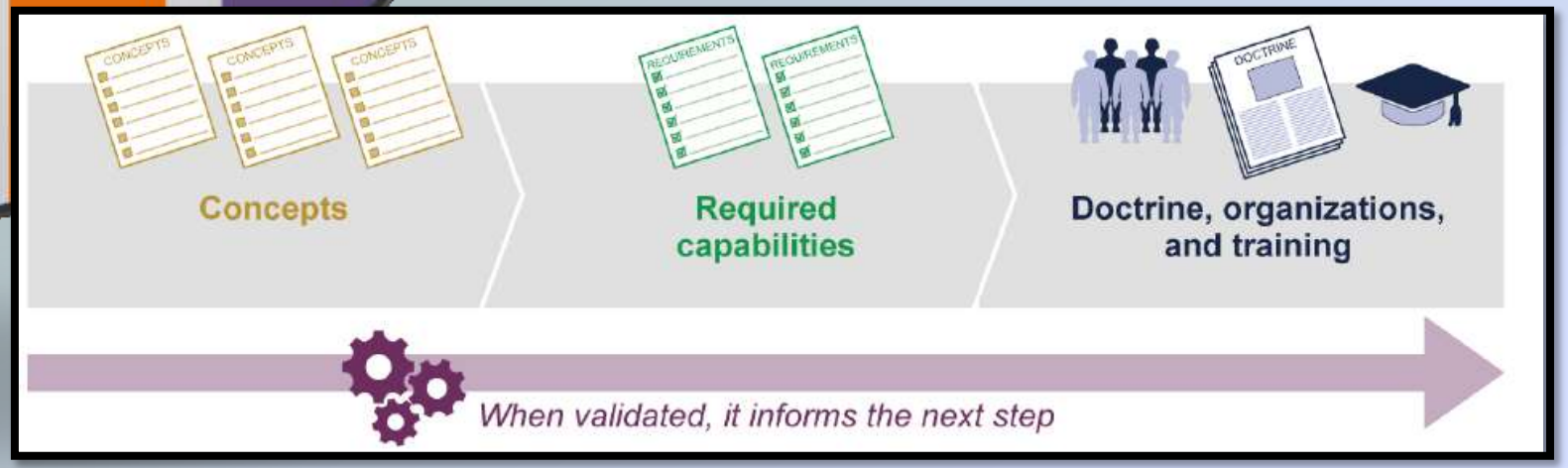


ADAPTED FROM PAPER TITLED 'ANTI FRAGILE ELECTRONIC WARFARE ' BY MARC LICHTMAN OF VIRGINIA TECH

CRYSTAL GAZING

CONCURRENT DEVP





Combat Capabilities

→ Precision Engagement
→ Non-kinetic Engagement
→ Squad Sensors
→ Squad Autonomy

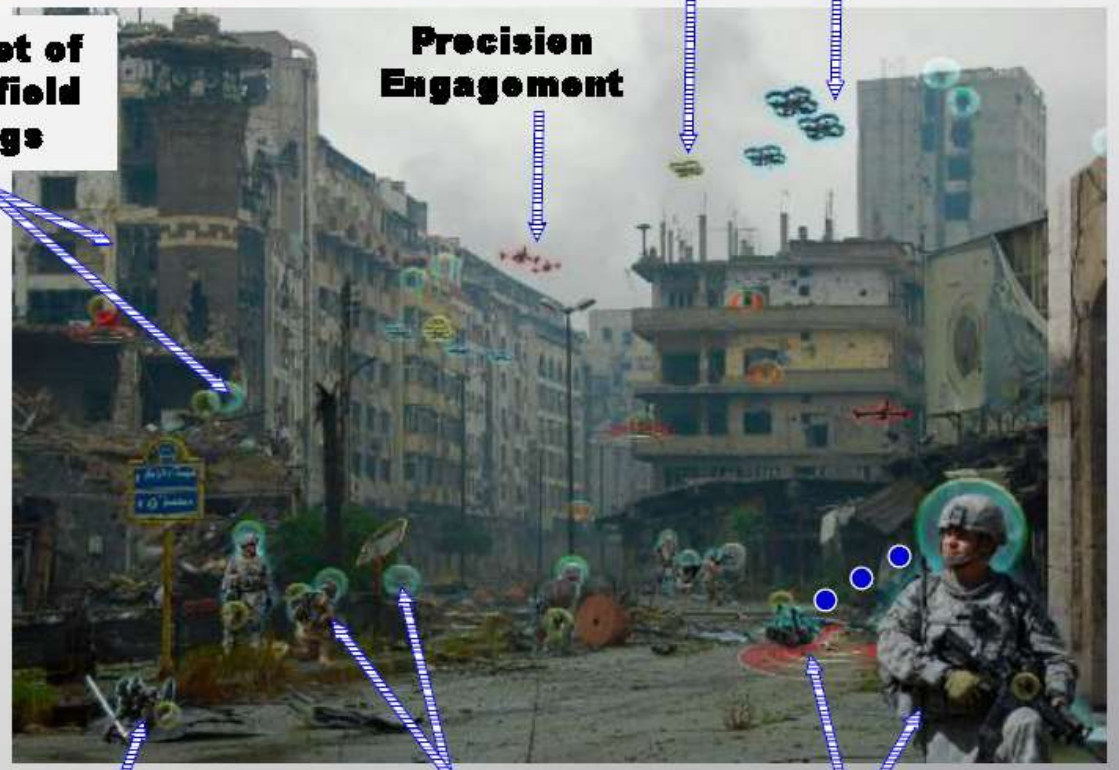
Autonomous UAV Swarms
→ ISR, force protection, BDA, network healing

Augmented Reality for Multi-faceted Picture →
operational environment, friend-foe locations, activities, threats

Cognitive EW & SIGINT

Internet of Battlefield Things

Precision Engagement



SIGINT/EW
→ sense adversaries, evade, jam

Personal Protection
→ counter cyber or electronic attack, signature management

Wearable Electronics
→ biosensors, threat locators, sensors

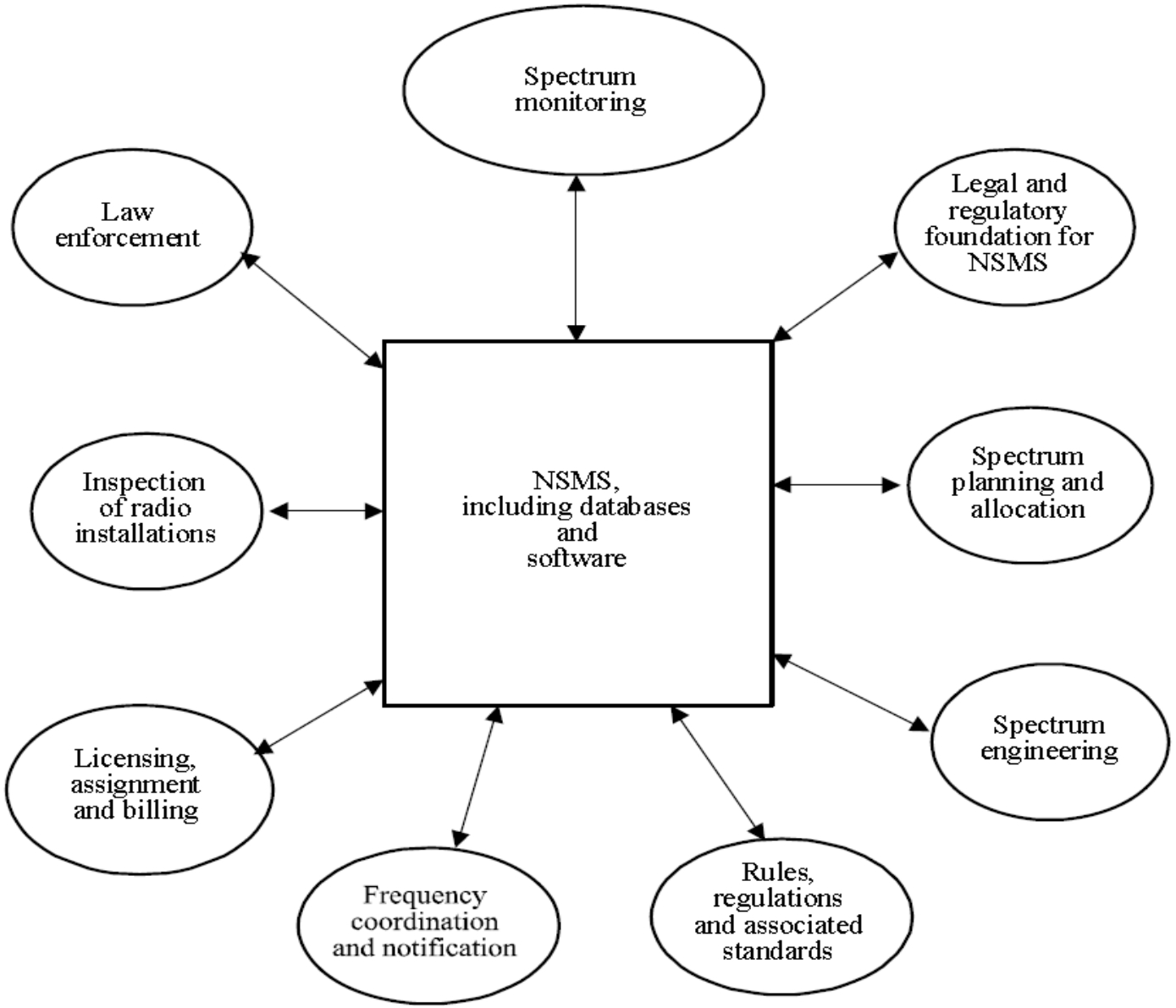
Net-enabled Semi-autonomous Weapons

Cognitive Networks
→ Network that perceives conditions, maintains memory, & adapts

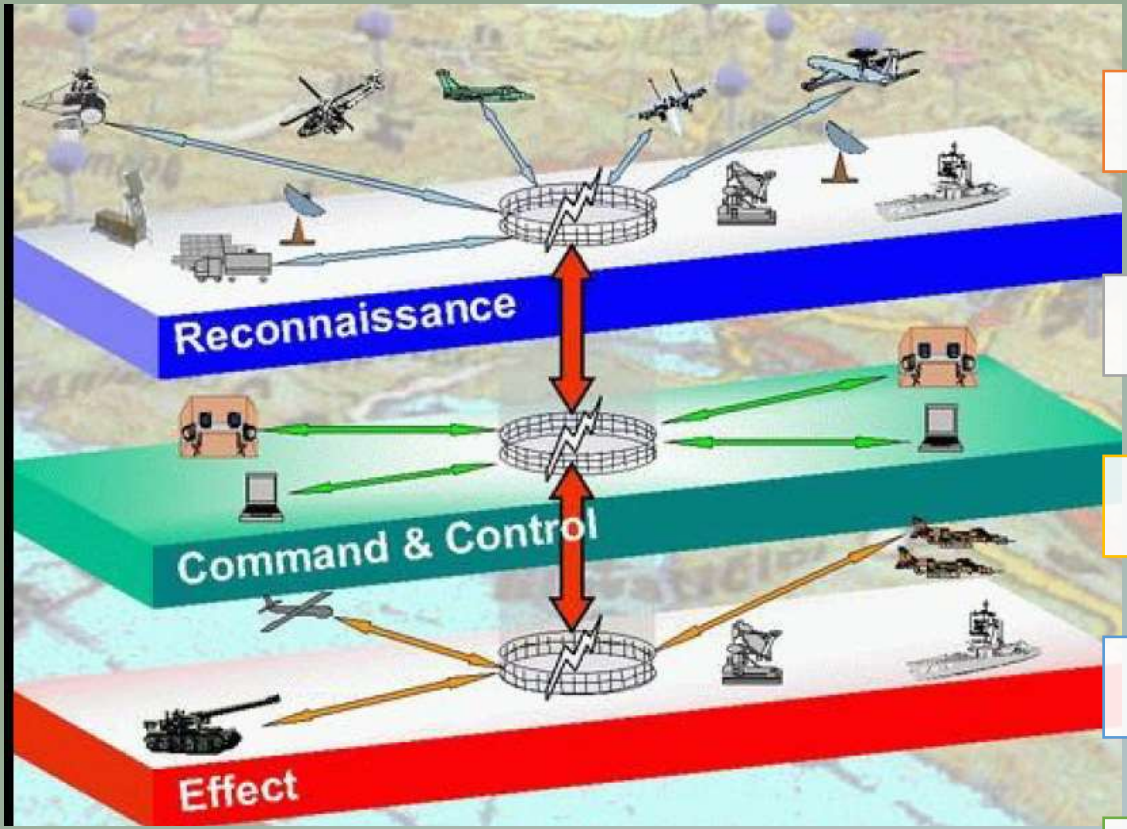
Human-Robot Combat Teaming
(e.g., Man Un-Manned Teaming)

Human-Machine Collaboration for Enhanced Decision Making

Simplified national spectrum management system



NATIONAL WAVEFORM DESIGN

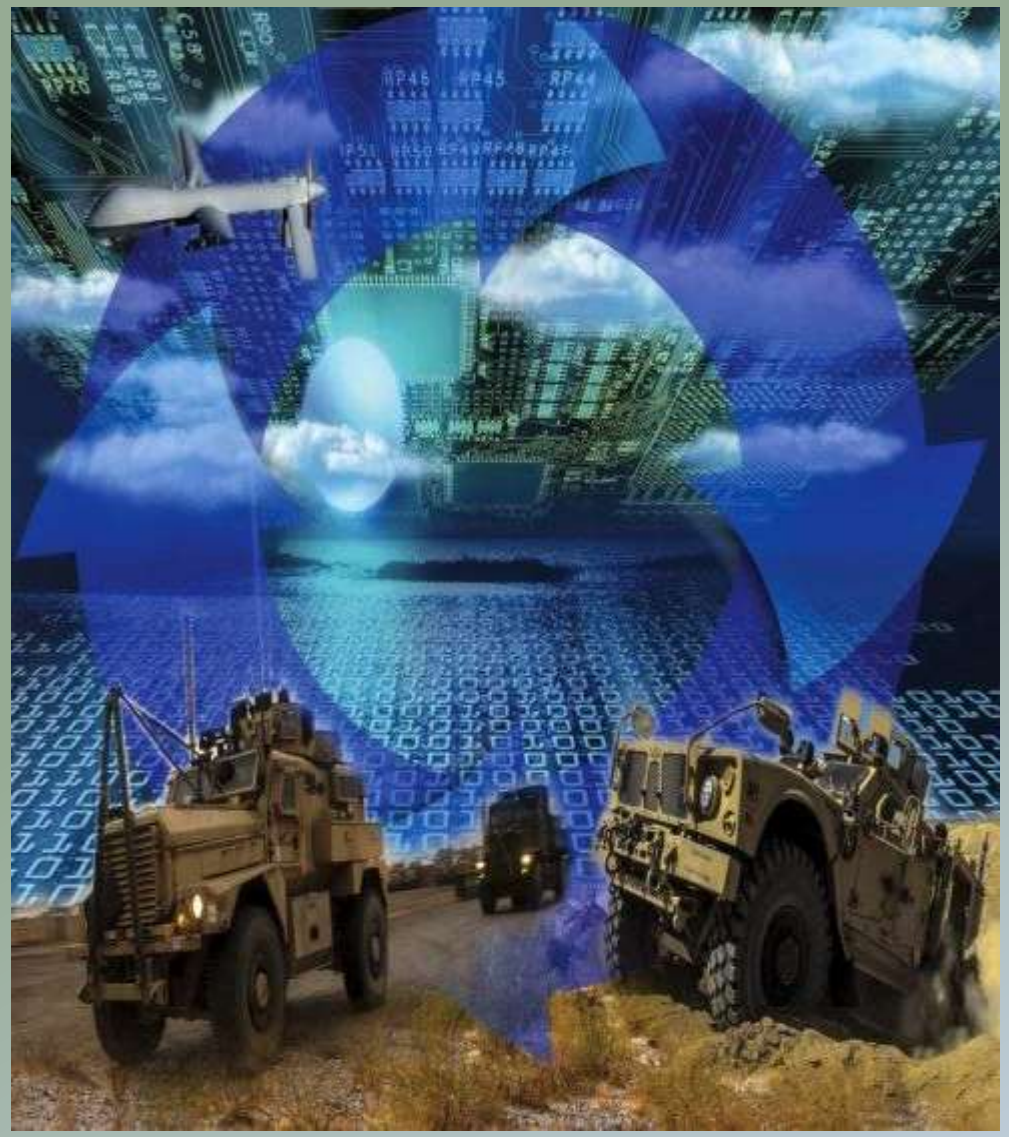


National Data Links: Waveform Design and its role in Modern Electronic Warfare operations

Hatim M. Behairy, Ph.D.
Associate Research Professor
Coordinator: Information and Communication Sector
Director: National Electronics, Communication and Photonics Center
King Abdulaziz City for Science and Technology

- COMMON WAVEFORM ACROSS ALL SERVICES – OWN DESIGN & DEVP
- SUPER IMPOSES ON TOP OF SERVICE SPECIFIC REQMT, IF ANY
- WE CAN ADD OWN SECRECY ACROSS ALL SERVICES – ECCM MEASURES UNIFORMITY
- OPTIMISE WAVEFORM FOR SPECIFIC TRN & GEO LOC
- USED ACROSS ALL AGENCIES IF NEEDED
- CONCURRENT DEVP & CONTER MEASURES DEVP

THE NEW BATTLEFIELD: THE RACE TO INTEGRATE CYBER AND ELECTRONIC WARFARE



WHY IS UNIFYING EM CAPABILITIES (SUCH AS EW, SIGINT, SPECTRUM MANAGEMENT, C4ISR AND NAVIGATION/ WAR) CURRENTLY SO IMPORTANT?

------ ENABLE SYSTEMS TO SCALE ACROSS PLATFORMS AND DOMAINS WHILE ENHANCING COMMONALITY & EFFICIENCY OF OPERATIONS AND THIS WILL EVOLVE TOWARDS AI-ENABLED MULTI-RF SYSTEMS.

SCALABILITY AND OPEN ARCHITECTURES WILL BE KEY TO ADDRESSING THESE DIFFERENT FACETS OF THE MODERN BATTLEFIELD.

A "ONE SIZE FITS ALL" SOLUTION WILL NOT WORK, AND THE ABILITY TO TAKE A CAPABILITY AND SCALE IT ACCORDING TO THE DIFFERENT NEEDS IS ESSENTIAL IF WE ARE TO MOVE AWAY FROM DESIGNING AD HOC SYSTEMS IN SILOS.

OPEN SOURCE ARCHITECTURE

Research Article

An Open Architecture Framework for Electronic Warfare Based Approach to HLA Federate Development

HyunSeo Kang,[1] **YoonJe Sung**,[1] **HyoungJun Kwon**,[1] **SugJoon Yoon**,[1] **and SangYeong Choi**[2]

[1]*Department of Aerospace Engineering, Sejong University, Seoul, Republic of Korea*
[2]*School of Defense Science, Hansung University and Myongji University, Seoul, Republic of Korea*

Correspondence should be addressed to SugJoon Yoon; sjyoon@sejong.ac.kr

Received 17 November 2017; Accepted 14 February 2018; Published 21 March 2018

OPEN ARCHITECTURE FRAMEWORK FOR ELECTRONIC WARFARE (OAFEW) HAS BEEN DEVELOPED FOR REUSABILITY OF VARIOUS OBJECT MODELS PARTICIPATING IN THE ELECTRONIC WARFARE SIMULATION AND FOR EXTENSIBILITY OF THE ELECTRONIC WARFARE SIMULATOR.

OAFEW IS A KIND OF COMPONENT-BASED SOFTWARE (SW) MANAGEMENT SUPPORT FRAMEWORK.

FUTURE REQMTS

- SUFFICIENT LOW NOISE CAPB IN THE RECEIVERS
- ABILITY TO OPERATE ACROSS WIDER BANDWIDTHS AND AT HIGHER FREQUENCIES WHILE GENERATING SUITABLE OUTPUT POWER IN THE TRANSMIT CHAIN
- SWaP CONSIDERATIONS TO INCL PORTABILITY, MODULARITY & SCALABILITY
- SOLID STATE SEMI CONDUCTORS – GaN IS HERE TO STAY
- COST FACTOR
- RELIABILITY

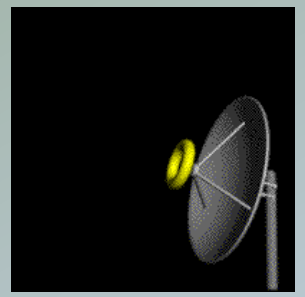
- DEALING WITH ROGUE ELEMENTS - ASYMMETRY
- CONVERGENCE OF FIELDS – COMPLEMENTARY EFFECTS
- SPECTRUM SENSING & SHAPING
- CHANGE IN THREAT ASSESSMENT – WAR TO BE WON EVEN BEFORE THE BATTLE IS FOUGHT

All warfare is based on deception . . . hold out baits to entice the enemy. Feign disorder, and crush him.

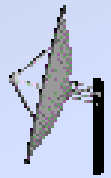
— Sun Tzu, *The Art of War*, 1.18–20

Force, and Fraud, are in warre the two Cardinal Virtues.

— Thomas Hobbes



NOTHING GOES UNNOTICED



ELECTRONIC WARFARE

THIS IS THE CONTEST for control of the electromagnetic spectrum, a battle fought in the domain of electronic warfare, or EW, and without it there can be no missi

EW TECHNOLOGY has advanced from the large format, lly developed in the late 1950s to the tware defined technology today. The pectrum dominance requires strategies that keep warfighters in he threat. Harris is innovating and f EW.

B-52
AN/ALQ-172
Analog
>500 lbs.

B-1B LANCER
AN/ALQ-161
Analog
>500 lbs.

FROM ANALOG:
Hardware Defined, Stove-Piped, Sta
Single Mission, Static Techniques

TO DIGITAL:
Software Defined, Modular, Networ
Multi-Function, Adaptive

TECHNOLOGICAL ADVANCEMENT

SIZE, WEIGHT AND POWER

NULKA
Digital
<10 lbs.

DISRUPTOR SRx™
Digital
<5 lbs.

OPEN ARCHITECTURE/ SOFTWARE DEFINED/ MISSIONIZED CAPABILITY

1960s **1970s** **2010s** **2020** AND BEYOND

ANALOG DIGITAL MODULAR SCALABLE OPEN