Review Peperangan Elektronika (*Electronic Warfare*)

Rustamaji
Teknik Elektro Institut Teknologi Nasional (Itenas)
Jl. P.H. H. Mustofa 23 Bandung 40124
Email : rustamaji@itenas.ac.id

ABSTRAK

Pada saat ini semakin banyak Negara-negara di dunia menyadari kenyataan terhadap keunggulan dari Electronic Warfare dan kebutuhannya dalam lingkungan pertempuran (combat environment). Terdapat dua kategori Electronic Warfare, yaitu : Passive Electronic Warfare dan Active Electronic Warfare. Tren yang berkembang saat ini dan masa datang adalah rancangan perangkat Electronic Warfare otomatis penuh, dengan mengintegrasikan antara active Electronic Warfare dan passive Electronic Warfare yang sesuai melalui interface dengan sensor dan sistem senjata lain. Electronic Warfare merupakan elemen penting pada konsep peperangan modern (modern warfare), digunakan dalam peperangan modern untuk menghadapi gangguan (interferensi) dalam bentuk gelombang elektromagnetik oleh lawan terhadap aliran komunikasi.

Kata kunci : *Electronic Warfare, passive, active*

1. PENDAHULUAN

Pada saat ini semakin banyak Negara-negara di dunia menyadari kenyataan terhadap keunggulan dari **EW = *Electronic Warfare*** dan kebutuhannya dalam lingkungan pertempuran (*combat environment*).

Semakin besar ketergantungan pada spektrum elektromagnetik sebagai sarana komunikasi, deteksi sasaran dan pengendalian senjata secara virtual untuk EW pada masa datang.

Rantai komunikasi, *radar*, detektor infra merah, *laser*, passive multi meter-wave radio meter, kamera televisi dan divais penglihat semuanya menggunakan sebagian dari spektrum elektromagnetik untuk beroperasinya.

Setiap sistem senjata modern yang ada saat ini ataupun yang sedang direncanakan menggunakan satu atau beberapa divais tersebut untuk melengkapi fungsinya sehingga misinya dapat berjalan secara efektif. Konsekuensinya, zona pertempuran modern akan penuh terisi dengan ribuan sinyal (pulsa) elektomagnetik.

Tujuan dari EW untuk mengeksploitasi lingkungan secara penuh ini, dinamakan *electronic battlefield* (medan pertempuran elektronika).

Terdapat dua kategori EW = *Electronic Warfare*, yaitu :

- *Passive EW* : Apabila digunakan perangkat yang secara pasif hanya mendeteksi atau memonitor energi dari sinyal-sinyal komunikasi atau sinyal elektronik lawan.

Teknik *passive EW* sering digunakan untuk mendapatkan informasi (*intelligence*) berharga.

- Memonitor komunikasi lawan dapat memberikan informasi berguna untuk saat itu dan perencanaan aktifitas.
- Pendeteksian secara pasif radar lawan, emisi laser dan infra merah dapat menyediakan peringatan dini (*early warning*) dan informasi untuk menyiapkan senjata.

- *Active EW* : Apabila digunakan perangkat yang secara aktif memancarkan energi (sinyal) untuk mendeteksi atau mengganggu sinyal-sinyal komunikasi atau sinyal elektronik lawan

Teknik *active EW* digunakan apabila dipertimbangkan untuk meniadakan atau mencegah lawan menggunakan spektrum elektromagnetik.

- Maka noise atau *deception jamming* (jamming penyesat) digunakan untuk mengacaukan (*disrupt*) atau mengganggu (*interfere*) jaringan *C3I (command, control, communication, and information)* dan sistem radar lawan.
- *Chaf* (lembaran logam), *infrared flares* dan *smoke* (asap) digunakan untuk membingungkan (*confuse*)

atau untuk menurunkan efektifitas *radar seeker*, *heat-seeking infrared seeker* dan sistem yang menggunakan laser atau divais optik.

Contoh nyata efektifitas penggunaan perangkat EW, terlihat pada :

- Penggunaan radar oleh pasukan Inggris untuk mendeteksi kedatangan pesawat pembom Jerman, sehingga pesawat pemburu Angkatan Udara Inggris (RAF) dapat mencegat pesawat Angkatan udara Jerman (Luftwafe) sebelum memasuki wilayah Inggris pada PD II (*Battle of Britain*).
- Penebaran *Chaff* secara besar-besaran pada saat serangan udara pesawat terbang Inggris (RAF) terhadap kota Hamburg pada Juli 1943.
- Perang Malvinas antara agresor Inggris yang tetap ingin menguasai kepulauan Malvinas dengan Argentina yang memilikinya. Dimana rudal Exocet yang diluncurkan oleh pesawat Super Etendard Argentina dibingungkan oleh *chaff* yang ditebarkan dari kapal HMS Hermes milik Inggris.
- Perang Yom Kippur antara Mesir melawan zionis Israel, dimana pada saat itu digunakan *jamming* oleh kedua belah pihak untuk mengacaukan jalur komunikasi masing-masing.
- Penggunaan pesawat EA-6 Intruder milik angkatan laut Amerika, yang di perlengkapi peralatan perang elektronika untuk mengacaukan dan melumpuhkan radar pertahanan udara Vietnam Utara. Sehingga pesawat-pesawat tempur Amerika leluasa memasuk wilayah udara Vietnam Utara.
- Perang teluk II, dimana pasukan agresor Amerika menggunakan rudal Patriot dan sistem radarnya untuk mendeteksi kedatangan serangan rudal Scud yang diluncurkan pasukan Irak, dan menghancurkannya.
- Penggunaan *passive radar* oleh pasukan Serbia dalam konflik Balkan, dimana kedatangan pesawat siluman F-117 Nighthawk milik Amerika yang akan melakukan pengeboman di wilayah Serbia dapat terdeteksi dan berhasil ditembak jatuh.

Tren yang berkembang saat ini dan masa datang adalah rancangan perangkat EW otomatis penuh, dengan mengintegrasikan antara *active EW* dan *passive* EW yang sesuai melalui *interface* dengan *sensor* dan sistem senjata lain.

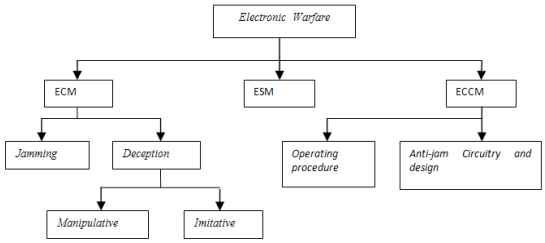
2. PEPERANGAN ELEKTRONIKA (EW *: ELECTRONIC WARFARE*).

Electronic Warfare (EW) umumnya disebut pula *Radio Electronic Combat* (REC) atau *Maskirovka* dalam istilah Rusia, merupakan elemen penting pada konsep peperangan modern (*modern warfare*).

Electronic Warfare (EW) dibagi menjadi tiga bagian yaitu :

- *Electronic counter measures* (ECM) atau kontra tindakan elektronika
- *Electronic counter-counter measures* (ECCM) atau kontra kontra tindakan elektronika, dan
- *Electronic-warfare support measures* (ESM) atau tindakan dukungan EW.

Gambar 1, menunjukkan struktur EW.



Gambar 1. Struktur EW (EW *tree)*

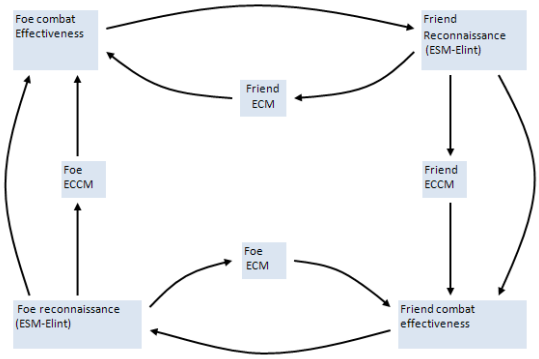
Di Amerika serikat, *electronic*, *communication and signal intelligence* (ELINT / COMINT / SIGINT) dan *electromagnetic compatibility* (EMC) tidak dimasukkan ke dalam struktur EW.

2.1. PENGERTIAN *ELECTRONIC WARFARE* (EW).

Electronic Warfare (EW) adalah pekerjaan militer pada energi elektromagnetik yang meliputi : Aksi yang diambil untuk menekan (*reduce*) atau mencegah (*prevent*) musuh (*foe*) menggunakan spektrum elektromagnetik; menjamin teman (*friend*) menggunakan spektrum elektromagnetik; dan menyergap (*intercept*), mengenali (*identify*), menganalisis (*analyze*), dan menemukan (*locate*) pancaran elektromagnetik musuh untuk mendukung ECM dan ECCM.

Electronic Warfare (EW) modern, dimulai pada perang dunia ke-2, dengan digunakannya secara intensif peralatan komunikasi elektronika dan Radar dari fihak sekutu maupun poros pada peperangan.

Skenario *Electronic Warfare* (EW), ditunjukkan pada gambar 2 berupa diagram interaksi antara elemen *Electronic Warfare* (EW) .



Gambar 2. Interaksi antara elemen *Electronic Warfare.*

Skenario melibatkan *friend* (teman) dan *foe* (lawan). *Friend* membangun jaringan komunikasi dan menjaganya tetap operasional.

Dalam operasinya *friend* menghadapi *electronic warfare* : dimana *foe* akan berusaha membangun *a set of measure* (langkah tindakan) untuk (*deny*) menyangkal atau meniadakan tujuan *friend*, atau akan menyadap (*tap*) saluran komunikasi dan membawa informasi dari *friend* ke dalam jaringannya.

Dalam situasi yang dinamis, diasumsikan kedua jaringan komunikasi *friend* dan *foe* bekerja dalam kondisi terbaik.

Friend mempunyai jaringan komunikasi dengan tujuan :

1. untuk membangun dan memelihara jaringan komunikasi
2. untuk melawan (*counteract*) setiap usaha *foe* untuk menghalangi atau memanfaatkan (*detect* : mendeteksi, *eavesdrop on* : mencuri dengar) aliran komunikasi.

Sedangkan terhadap *friend, Foe* mempunyai kesempatan :

1. untuk *detect* dan atau *localize* (menentukan lokasi) keberadaan link komunikasi , dengan
2. to *eavesdrop on* aliran informasi
3. *to block* aliran informasi dengan (*jamming* : pemacetan)
4. *to insert* (menyusupkan) informasi salah (*spoofing*)
5. memilih strategi baru, apabila apabila ada kontra tindakan (*countermeasures*) oleh pemilik jaringan.

Apabila interaksi kedua sistem *friend* dan *foe* semakin meningkat : komunikasi atau tindakan elektronika (EM : *electronic measure*) akan diikuti kontra tindakan elektronika (ECM : *electronic countermeasure*), ini akan memicu kontra kontra tindakan elektronika (ECCM : *electronic counter countermeasure*), dan seterusnya seperti digambarkan berikut :

Action by friend *Action by foe*

EM

ECM

ECCM

$EC^{n-1}M$

$EC^{n}M$

$EC^{n+1}M$

Faktor yang membatasi dalam proses ini adalah waktu dan biaya, dalam hal ini adalah teknologi.

Terlihat dari skenario diatas, fihak yang menguasai teknologi akan lebih unggul dalam peperangan elektronika.

2.2. *ELECTRONIC COUNTER MEASURE* (ECM).

Teknik ECM : *Electronic counter measure* atau kontra tindakan elektronika, dapat di klasifikasikan dalam sejumlah cara antara lain:

- dengan "*basic" purpose*,
- kondisi *active or passive*,
- dengan *waveform*
- dengan *deployment / employment*
- dengan *combination of way*

Tidak ada cara yang khas untuk mengklasifikasikan teknik ECM, dimana pengaruh ECM dapat dilihat pada tabel 1.

Dimana *Jamming* adalah bagian dari *Electronic counter measures* (ECM), seperti terlihat pada gambar 1.

Jammer dapat ditempatkan di darat, diatas kapal atau pada pesawat terbang. Metoda penyebaran melalui udara (*airborne deployment*) meliputi :

- *self-screening jamming* (SSJ) – jammer dibawa oleh pesawat terbang penyerang / *attacking aircraft*.

- *escort jamming* (ESJ) – jammer dibawa oleh pesawat terbang yang mengiringi pesawat terbang penyerang, yang sering disebut "*quiet aircraft*".
- *stand-off jamming* (SOJ) – jammer dibawa pesawat terbang khusus yang terbang di orbit diluar jangkuan mematikan pasukan pertahanan
- *expendable jamming* (EJ) - jammer dijatuhkan atau dilontarkan di dekat radar musuh

Terdapat dua kegunaan dasar ECM :

- *denial* atau penolakan atau penyangkalan
- *deception atau* penyesatan.

Sedangkan tipe-tipe ECM dapat dilihat pada tabel 2.

Pada *denial* ECM, kemampuan *receiver* lawan untuk menerima pesan atau untuk mendeteksi sasaran (*target*) diserang dan *receiver* lawan akan loncat (*hopping*), turun (*degrade*) atau kalah (*defeat*). Denial ECM sering disebut juga melakukan *active jamming* pada atau dekat frekuensi operasi *radar* atau *radio receiver* lawan yang menjadi sasarannya.

Berbagai bentuk gelombang (*waveform*) *jamming* dapat digunakan antara lain :

- *Broadband noise jammer*
- *Partial-band noise jammer*
- *CW (Continuous Wave) jammer*
- *Multitone jammer*
- *Pulse jammer*
- *Repeat-back jammer*

Pada *deception* ECM, sinyal palsu (*spoofers*) digunakan untuk mengacaukan atau membingungkan operator *radar / radio receiver* lawan.

Meliputi komunikasi palsu (*false communication*), *dummy reflector target*, *false electronic target*, *erroneous radar beacon replies*, dan *erroneous target angle modulation.*

Chaff adalah termasuk dalam *passive deception* ECM yang penting, sejak digunakan pertama kali secara besar-besaran pada saat serangan udara pesawat terbang Inggris (RAF) terhadap kota Hamburg pada Juli 1943.

Memperkecil *radar cross section* adalah cara lain *passive denial / deception* ECM. Dengan memperkecil *radar cross section* akan menurunkan jarak jangkau deteksi radar lawan, tanpa harus mengoperasikan *active jamming*. Juga akan menurunkan banyaknya *chaff* yang dibutuhkan untuk melindungi pesawat.

2.3. *ELECTRONIC COUNTER COUNTER MEASURE* (ECCM).

Teknik ECCM adalah cara yang digunakan (*powerful mean*) untuk menurunkan pengaruh ECM atau ESM oleh kekuatan lawan. Pengaruh ECCM dapat dilihat pada tabel 3.

Pengaruh ECCM yang terakhir, yaitu CESM (*counter*- ESM) dapat sangat berguna dalam mencegah atau menunda inisiasi pemilik ECM, sehingga memungkinkan *radar* bekerja sesuai dengan waktu yang direncanakan.

Teknik CESM meliputi dua kategori dasar, yaitu : *Low probability interception* dan *Low probability identification.*

Pada saat yang sama teknik CESM juga dapat memberikan keuntungan lain ECCM.

Terdapat beberapa cara mengklasifikasikan teknik ECCM, antara lain berdasarkan:

- keuntungannya
- prioritas teknik pada sistem radar
- fungsi dasarnya
- tipe ECM yang digunakan

sedangkan pentingnya ECCM dapat dilihat pada tabel 4.

2.4. ELECTRONIC WARFARE SUPPORT MEASURES (ESM).

ESM didefinisikan sebagai pemberian dukungan baik kepada ECM maupun ECCM.

Kebanyakan Fungsi ESM dalam mendukung ECM telah dikenal seperti dapat dilihat pada tabel 5, dan ditunjukkan oleh peralatan *radar homing and warning* (RHAW), *intercept receiver* dan lain-lain.

Kebanyakan *modern jammers* meliputi fungsi *intercept receiver*, untuk menempatkan *jammer* pada frekuensi *receiver* lawan yang jadi korbannya.

ESM juga meliputi fungsi identifikasi sinyal (*signal dentification*) dan pengujian ancaman (*threat assessment*).

Ini sangat penting untuk menentukan apakah sinyal akan di-jamm atau tidak di-jamm untuk *communication traffic interception.*

Meskipun ESM dalam mendukung ECCM kurang dikenal dari pada ESM dalam mendukung ECM, tetapi perlu diperhatikan.

Seperti dapat dilihat pada tabel 6.

Fungsi yang ditunjukkan pada tabel 6, aplikasi utamanya pada *radar.*

Teknik ECCM radar dari *frequency agility* yang popular saat ini, meningkat secara cepat oleh karena penggunaan *integral intercept receiver* untuk memonitor frekuensi transmisi *radar*, bila memungkinkan untuk mencegah *jamming*.

3. KESIMPULAN.

Sesuai dengan pengertian atau fungsi EW : *Electronic Warfare* (EW) adalah pekerjaan militer pada energi elektromagnetik yang meliputi :

- Aksi yang diambil untuk menekan (*reduce*) atau mencegah (*prevent*) musuh (*foe*) menggunakan spektrum elektromagnetik;
- Menjamin teman (*friend*) menggunakan spektrum elektromagnetik; dan
- Menyergap (*intercept*), mengenali (*identify*), menganalisis (*analyze*), dan menemukan (*locate*) pancaran elektromagnetik musuh untuk mendukung ECM dan ECCM.
-

DAFTAR REFERENSI

[1] International Defense Review Magazine - Electronic Warfare

[2] The Intelligence War Book

[3] Military Technology Magazine - Electronic in Defence

[4] Defences Electronic Book - The Electronic Navy

[4] Doug Richarson - Electronic warfare

[5] R, Skaug, J.F. Hjelmstad – Spread Spectrum In Communication

[6] Rustamaji Tugas akhir, “Video Scrambling System”, ITENAS, 1990.

[7] Rustamaji Tesis, “Perancangan Model Perangkat Frequency Hopping “, ITB, 1998.

[8] Rustamaji Artikel ilmiah, “Membuat Telekomunikasi Antisadap”, REPUBLIKA, 16 April 1999.

[9] Rustamaji Artikel ilmiah, “Awas, Jaringan Komunikasi Pemilu Direkayasa”, REPUBLIKA, 6 Juni 1999.

[10] Rustamaji Artikel ilmiah, “Melacak Buronan Dengan Voice Analyzer”, REPUBLIKA

[11] Rustamaji, Elan Dj ,“Penggunaan Teknik Spread Spectrum Pada Electronic warfare”.

[12] Rustamaji, Elan Dj, “ Penggunaan Teknik Direct Sequence - Spread Spectrum Pada Electronic warfare”.

[13] Rustamaji, Elan Dj. ”Aplikasi Rangkaian Terintegrasi Direct Digital Syntheziser (DDS) Sebagai pembangkit Sinyal Frequency Hopping Spread Spectrum (FHSS)”,

[14] Rustamaji Tugas akhir, “Video Scrambling System”, ITENAS, 1990.

[15] Rustamaji Tesis, “Perancangan Model Perangkat Frequency Hopping “, ITB, 1998.

[16] Penelitian Program Kompetitif LIPI, “Pemancar dan Penerima Frequency Hopping Spread Spectrum Untuk Pengamanan Sinyal Informasi”, LIPI, 2004-2006.

[17] Penelitian Kerjasama TNI-AL, LIPI dan Itenas, ”Broad band Radio jammer Komunikasi VHF Low Band”. LIPI 2006.

[18] Program Insentif MENRISTEK, ” Realisasi Perangkat VHF Electronic Jamming Untuk Elecktronic Warfare”, 2007-2008

[19] Rustamaji; Elan Djaelani, ‘Pemancar Frequency Hopping Spread Spectrum Untuk Pengamanan Sinyal Informasi”, Jurnal Teknologi Informasi LIPI, Vol 3 no 1, 2002.

[20] Rustamaji; Elan Djaelani, ‘Frequency Hopping Spead Spectrum Suatu Teknik Pengamanan Komunikasi Pada Perang Elektronika (Electronic Warfare)”, Prosiding, Pemaparan Hasil Litbang 2003 LIPI, 2003

[21] www.wikipedia.com