Pengenalan Peperangan Elektronika (*Electronic Warfare*)

Elan Djaelani
Pusat Penelitian Informatika, LIPI
elan@informatika.lipi.go.id

Rustamaji
Teknik Elektro-ITENAS
rustamaji@itenas.ac.id

Abstrak

Pada saat ini di Pusat Penelitian Informatika telah dilaksanakan penelitian dengan topik topik bidang pertahanan dan keamanan, seperti Steganografi,Radio Frequency Hopping,Telepon Scrambler,Scrambler Descrambler Morse, Radio Jamming dan yang lainnya.Puslit ini mendukung penerapan komputer,mikrokontroler, interface, dan software untuk pertahanan dan keamanan.

Merupakan salah satu topik bidang pertahanan lainnya adalah peperangan elektronika, merupakan pekerjaan militer pada penguasaan gelembang elektro magnetic.Pada perang modern ini peran peperangan elektronika sangat penting, dan melalui makalah ini penulis akan memperkenalkan tentang peperangan elektronika.

Kata kunci: peperangan elektronika

1. Pendahuluan

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

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

Rantai komunikasi, radar, detektor infra merah, laser, passive multimetre-wave radio metre, 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 :

1. *Passive EW*

Teknik EW pasif (*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.

2. *Active EW*

Teknik EW aktif (*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), Electronic counter-counter measures (ECCM), dan Electronic-warfare support measures (ESM) Gambar dibawah ini menunjukkan struktur EW.

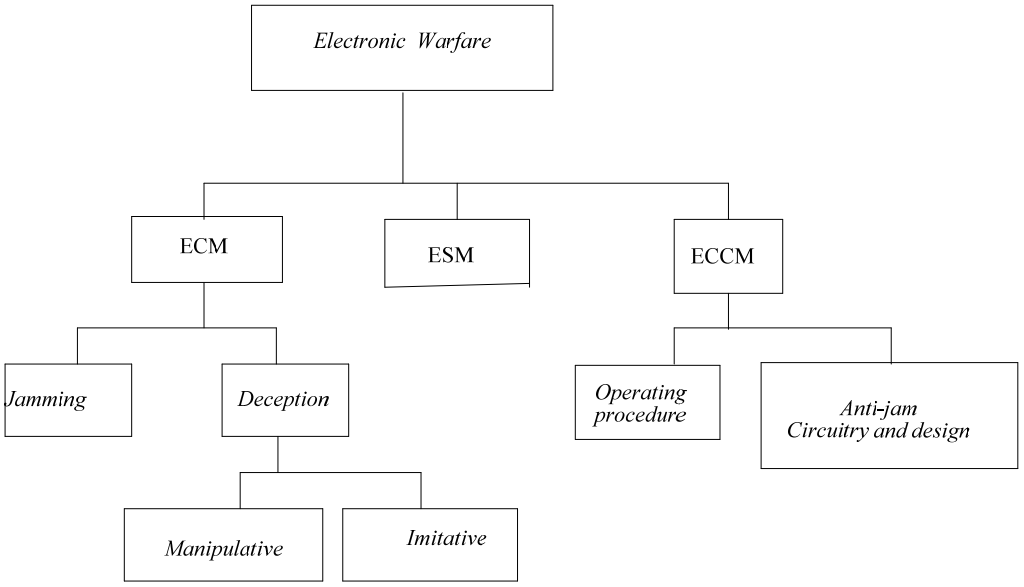
Dimana Jamming adalah bagian dari Electronic counter measures (ECM), seperti terlihat pada gambar 1.

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

3. Pengertian *Electronic Warfare*

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 pihak sekutu maupun poros pada peperangan.



Gambar 1 Struktur EW (*EW tree*)

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

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:

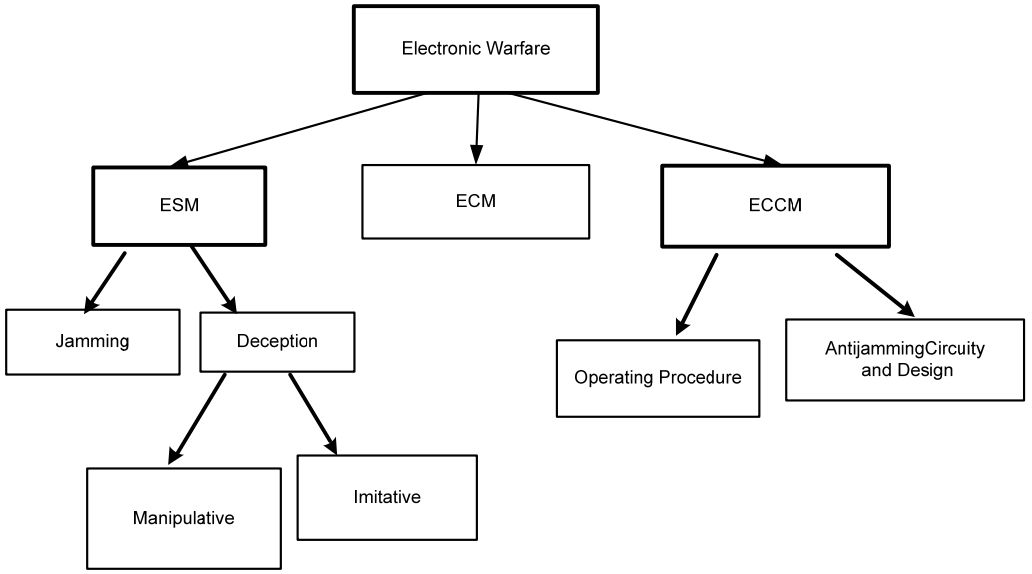
1. untuk membangun dan memelihara jaringan komunikasi
2. untuk melawan (counteract) setiap usaha foe untuk menghalangi atau memanfaatkan (detect : mendeteksi, eavesdrop on : mencuri dengar) aliran komunikasi.

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-1M
EC nM	
	EC n+1M



Gambar 2 Interaksi antara elemen Electronic Warfare

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.

4. Topik-Topik Penelitian *Electronic Warfare*

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.

Dapat dikelompokkan beberapa topik untuk penelitian .

1. *Radar*: Pulse radar, CW radar, antennas (*aerials*), *Surveillance radar, Frequency- hopping radar, Travelling wave tube, Pulse-doppler radar, Flat-plate antennas, Electronic noise*
2. *Millimetre wave*
3. *Infra red: Heat seeking missiles, imaging infra red*
4. Electro optical system
5. *Sonar: Sonar platforms, Towed arrays, Sonobuoys, Seabed sonar*
6. *Stealth technology: Non reflective materials, Countour control, Radar-absorbent materials, RCS reduction, Thermal signature reduction, Emission suppression*
7. *Electronic intelligence gathering: Tactical and strategic sigint, Sigint organzations, Comint, Comint targets, Speech recognition, Radiaton intelligence, Geopolitical interference, Signal analysis, Bluff and counter bluff, Lunar reflector*
8. *Counter measure*
9. *Warning receiver and ESM system: Countering guideline, Threat detection, Tracking indication,*
10. *ESM System: Signal analysis, Millimeter wave system, IR warning*
11. *EW expendables: Chaff, Flare, Smoke & Decoy*

12. *Active Jamming: Noise jamming, Spot jamming, Barrage jamming, Deception Jamming*
13. *Infra Red, Electro Optic and Sonar Jamming*
14. *Radio Spread Spectrum : Frequency hopping, Time hopping, Direct sequence, Chirp.*
15. *Anti-radar Weapon and Aircraft: Anti radiation missile*
16. *Electromagnetic Pulse: Radiation hardening, EMP-resistant microchips, Hardened command posts, Harness testing.*
17. *Unconventional Threats: Electronic virus, EM bom, Hacking, Information security (PIN, Pasword, DES, encryption, chipering, scrambling, spectrum shifter, spectrum inversion, amplitude inversion).*

4. Kesimpulan

Topik topik penelitian diatas dalam pelaksanaannya memerlukan multi disiplin ilmu, termasuk diantaranya teknologi computer atau teknologi informasi dan komunikasi.

Puslit Informatika dapat berperan pada penelitian ini.Penelitian ini memerlukan sumber daya manusia yang memadai baik jumlah dan kualitasnya.Pembentukan Sumber Daya Manusia (SDM) yang diperlukan dilaksanakan melalui program sekolah, pelatihan ataupun ikut seminar nasional dan internasional.

5. Daftar pustaka

[1] International Defense Review - Electronic Warfare
[2] Intelligence War
[3] Military Technology - Electronic in Defence
[4] Defences Electronic - The Electronic Navy
[5] Doug Richarson - Electronic warfare
[6] R, Skaug, J.F. Hjelmstad – Spread Spectrum In Communication
[7] Marvin K. Simon etc – Spread Spectrum Communication
[8] Laporan Akhir Program Insentif MENRISTEK, ” Realisasi Perangkat VHF Electronic Jamming Untuk Elecktronic Warfare”,2008
[9] Rustamaji; Elan Djaelani, ‘Pemancar Frequency Hopping Spead Spectrum Untuk Pengamanan Sinyal Informasi”, Jurnal Teknologi Informasi LIPI, Vol 3 no 1, 2002.
[10] Rustamaji; Elan Djaelani, ‘Frequency Hopping Spead Spectrum Suatu Teknik Pengamanan Komunikasi Pada Perang Elektronika (Electronic Warfare)”, Prosiding, Pemaparan Hasil Litbang 2003 LIPI, 2003
[11] Ulrich L, Rohde; T T N Bucher,”Communication Receiver : Principles and Design”,McGraw Hill.