Steven P. Winterfeld
Winterf001
GSEC
GSEC Practical Requirements (v.1.3) (December 2001)
Original submission
SANS Peachtree

Summary: This article will address the need for the US Army to apply its Intelligence Preparation of the Battlefield (IPB) doctrine to cyber space. FM 34-130 defines IPB as the systematic, continuous process of analyzing the threat and environment in a specific geographical area. It consists of Defining the battlefield environment, Defining the battlefield effects, Evaluating the threat (enemy) and Determining threat courses of action (COAs). This article will cover the current doctrine and how to apply this doctrine to cyber space or if there is a need to completely overhaul the doctrine.

CYBER IPB

The US Army has made great efforts to automate the Intelligence Preparation of the Battlefield (IPB) process but has made little effort to apply IPB to the digital environment. The Army needs to develop this capability before it finds itself in a cyber war. This article will cover the current doctrine and how to apply this doctrine to the cyber space or completely overhaul the procedure. It will be technical in nature and not cover legal issues or organizational constraints, which are beyond the scope of this article.

Some would argue that the United States is engaged in cyber warfare already. Osama bin Laden and his associates' hid encrypted plans on the terrorist attack against the United States in pictures on the web and comments in chat rooms. [i] Soon after his 9/11 attack a hacker war started between a group calling itself Young Intelligent Hackers Against Terror (YIHAT) led by a young German vs. who took on Gforce (Pakistani lead anti-US group). [ii] The main activity was web page defacement but the primary target for Gforce was US military and government pages making U.S. cyber space the front lines.

Intelligence Preparation of the Battlefield (IPB): is defined as the systematic, continuous process of analyzing the threat and environment in a specific geographical area. It consists four steps (1) Defining the battlefield environment, (2) Defining the battlefield effects,(3) Evaluating the threat (enemy) and (4) Determining threat courses of action (COAs). [iii]

Current defining the battlefield environment process:

- Identify significant characteristics of the environment.
  - Type of environment will influence the intelligence required (urban, desert, tropical…).

    - Initial requirements: Gather available map sheets, country studies, history of the environment, demographics, ethnic issues, economics, trade, religion, and operation-specific information.
    - Type of operation / conflict will also affect intelligence requirements (drug interdiction, peacekeeping, or war).
- Identify the limits of the command's Area of Operations (AO) and battlespace. The AO is a geographical area assigned to the unit from higher headquarters. Battlespace includes both ground and air.
- Establish the limits of the Area of Interest (AOI). Usually determined as any enemy forces that could affect the AO within 72 hours.
- Identify amount of detail required / feasible within time available for IPB. The more time, the more detail. IPB never stops; it is an ongoing process.
- Evaluate existing databases and identify intelligence gaps. This will drive collection plans.
- Collect the information and intelligence required to conduct next IPB step.

This step in the IPB process is designed to start t0 produce the products needed for COA development. These products are: Priority Intelligence Requirements (PIR) focus collection assets on holes in the intelligence database and Request For Information (RFI) are key questions to higher headquarters that the unit doesn't have collection assets that will work. Next comes the Modified Combined Operations Overlay (MCOO), which reflects all the terrain and weather analysis. The doctrinal template (standard enemy tactics, doctrine and formations) is applied to the MCOO creating the event template. The event template shows named areas of interest, high value targets, and the decision support template. Finally a collection management plan is developed and given to subordinate units for execution. Link diagrams and pattern analysis graphs can be made to show relationships within the AOR depending on the type of conflict. As information is collected, the situation map is created showing real-time battlefield developments. All of these products combined allow the intelligence officer to conduct predictive analysis for the commander.

Current defining the battlefield effects process:

- Analyze the battlefield environment:
    - Terrain is analyzed using the following factors: Observation / fields of fire, cover and concealment, obstacles, key terrain (anything which gives one side a significant advantage), avenues of approach (OCOKA).
    - Weather is analyzed using the following factors: Visibility, winds, precipitation, cloud cover, humidity, temperature.
- Analyze other characteristics of the battlefield:
    - Telecommunications and computer infrastructure, nuclear–biological–chemical facilities, economic, political, legal, religious, race, culture, or any other demographics that effect the population.

This step in the IPB process is designed to provide the commander with a thorough understanding of the impact of terrain and weather will have on the battle. These factors provide a method of handling the information that must be analyzed and presented in a short amount of time. They have different levels of importance depending on the situation and forces involved so the process is very dynamic.

Current evaluating the threat (enemy) process:

- Disposition (Location)
- Composition (Organization and equipment)
- Strength (Percentage of forces combat mission capable)
- Recent, present and significant events or activities
- Peculiarities and weaknesses
- Capabilities
    - Most likely enemy COA (may have branches and sequels)
    - Most dangerous enemy COA to US forces
- Conclusions (effects on AO and enemy vulnerabilities)

This step provides a standard format for the commander to develop a rapid understanding of the enemy and defines the enemy for COA development. The problem is the formula was designed to analyze a conventional force, not a virtual force. With the advent of asymmetrical and asynchronous warfare (see definitions below) the battlefield no longer has a forward edge and a rear echelon. On this new battlefield a small anonymous group can have a disproportionate effect using weapons of mass effect by causing the public to have a loss of confidence in the economy (9/11 attack effected New York Stock Exchange) or national health system (Anthrax mail scare). These same principles can be applied to the United States Critical Information Infrastructure. It is important to point out that weapons of mass effect (WME) are different from weapons of mass destruction (WMD) because they are fully scalable.

Asymmetrical Threat: A threat that uses dissimilar weapons or force (e.g. WMD, small-scale attacks, information attack) to offset a superior military force and technological advantage. [iv]

Asynchronous Threat: A threat that doesn't require the orchestration of timing or simultaneous use of its capabilities to achieve a desired effect. Therefore causing haphazard attacks that result more on circumstance and personality rather than by a well-designed operation. (e.g. A terrorist faction that is structured by separate cells branched off for anonymity purposes acting independently of a primary leader of the faction.) [v]

Threats come from a range of sources from individuals (unauthorized users or insiders) to complex national organizations (foreign intelligence services and adversary militaries). Boundaries between these groups are indistinct, and it

is often difficult to discern the origins of any particular incident. For example, actions that appear to be the work of hackers may actually be the work of a foreign intelligence service. Sources include unauthorized users, insiders, terrorists, non-state groups, foreign intelligence services, and opposing militaries or political opponents. [vi]

Current determining threat Courses Of Action (COAs) process:

- Identify the threat's likely objectives and desired end state.
- Identify the full set of COA's available to the threat. The most likely and most dangerous should be developed at a minimum.
- Develop COA's based on enemy perception of friendly dispositions (reverse IPB).
- Evaluate and prioritize each enemy COA.
- Continue to refine COA as time and new information allow.

This step is the summation of the process and predicts what the enemy will do. This prediction is what friendly plans are based on. Most of the industrial countries have already publicly declared information operations and cyber warfare development programs. Major General Wang Pufeng of China says, "In the near future, information warfare will control the form and future of war. We recognize this developmental trend of information warfare and see it as a driving force in the modernization of China's military and combat readiness. This trend will be highly critical to achieving victory in future wars." [vii] Now let's look at what IPB is, how it is used, and where we need to go to provide predictive analysis to the warfighting commander.

Defense Secretary Donald Rumsfeld said, "A likely surprise attack in the coming years makes it imperative that the U.S. military undergo a transformation, starting now, in the way that it thinks, fights and manages itself." He enumerated six goals for transforming U.S. defense strategy and force structure: Protect both the U.S. homeland and U.S. bases overseas; Project and sustain power in distant regions; Deny sanctuary to America's enemies, no matter how remote, or mountainous or deeply dug in; Protect U.S. information networks; Use information technology so that different kinds of U.S forces can fight jointly; Maintain unhindered access to space. [viii]

The traditional doctrine has been the two major theaters of war policy. As a global power with worldwide interests, the United States must be able to deter and defeat two nearly simultaneous, large–scale, cross–border aggression in distant theaters in overlapping time frames, preferably in concert with regional allies. For the time being, we face this challenge in the Arabian Gulf region and in Northeast Asia. This is often in direct conflict with the reality of the need to conduct multiple, concurrent smaller-scale contingency operations. US military forces provide a full array of capabilities that can be tailored to give the National Command Authority (NCA) many options in pursuing our interests. Our capacity

to perform shows of force, limited strikes, opposed interventions, no-fly zone and sanctions enforcement operations, interposition or observation operations, and other missions allows us to deter would-be aggressors and control the danger posed by rogue states. US forces can also perform peace operations and humanitarian assistance operations, and can evacuate noncombatants from dangerous situations, whether opposed or unopposed. [ix] All of these operations depend on information dominance for success, which means better and faster intelligence.

Cyber space defining the battlefield environment process:

- Identify significant characteristics of the environment.
    - Classification of network: World Wide Web (WWW), Unclassified or Non-secure Internet Protocol Routing Network (NIPR – all .mil addresses), Secret or Secret Internet Protocol Router Network (SIPR) and Top Secret or Joint Worldwide Intelligence Communications System (JWICS) networks.
    - WANs, LANs, services, Database, Applications (Email), OS (Windows, Unix, Linux) and most importantly the actual information.
    - Baseline activity on network.
    - Architecture, operating systems, services.
    - Connectivity and bandwidth.
- Identify the limits of the network to be collected against.
- Establish the limits of the supporting or connected networks that may need to be collected against.
- Evaluate existing databases and identify intelligence gaps.
- Use non-military open source and international organizations to gather public information.

As the environment is analyzed the type of conflict will drive the process. The entire spectrum of engagement includes: Major Theater of War (MTW), Operations Other Than War (OOTW), Small Scale Contingency (SSC), and Stabilization and Support Operations (SASO) the control of information will play a larger part in determining the winner. We also need to understand the battlefield will no longer only include tactical networks but as we continue to leverage reach-back capabilities garrison networks will become mission critical.

This step produce similar products: PIR (still need to focus collection assets on what information we need for planning), understanding of network topologies, operating systems, services and applications as they apply to the area of interest, key systems template with high value systems and decision triggers for actions, collection management plan for both automated systems (bots – small programs that search out info and report back) and our hackers. Finally network diagrams and traffic analysis charts to present the analysis to the warfighter in an understandable format.

Cyber space defining the battlefield effects process:

- Analyze the battlefield environment: (Information, services and networks).
  - Confidentiality, integrity, availability (CIA)
  - Protect, detect, respond, restore and conduct reviews
- Analyze other characteristics of the battlefield:
  - Security
  - Auditing procedures
  - Backup systems

As the Army integrates off-the-shelf technology into military operations, it will require new skills and thought processes. We will need network analysis tools to discover topology, forensics tools to look at user behavior, risk analysis tools, and network-monitoring tools to get a common operational picture of both enemy and friendly network health. This is a good time to point out that there is no silver bullet solution. Despite the proliferation of technology and globalization of the threat it still comes down to well trained quality people. If cyber IPB is introduced now the Army can "train as you fight".

Cyber space evaluating the threat (enemy) process:

- Physical location of all assets
- Architecture and automation skills
- Security and policies
- Baseline activity
- Peculiarities and vulnerabilities
- Capabilities
  - Most likely COA
  - Most dangerous COA
- Conclusions that address: Rules of engagement (ROE) for Information Assurance (IA), Computer Network Defense (CND) and Computer Network Attack (CNA).

The goal of this phase of IPB is to predict the enemy's plan. Knowing where enemy reconnaissance forces would be and where the counter attack would come from allows the operations section to develop friendly COAs to defeat him. Sun Tzu said, "One who knows the enemy and knows himself will not be in danger in a hundred battles. One who does not know the enemy but knows himself will sometimes win, sometimes lose. One who does not know the enemy and does not know himself will be in danger in every battle." [x]

This requires doctrine on the types of threats, types of attacks, objectives and force protection measures. First categories of threats: internal (disgruntled or incompetent employee), external (hacker / cracker), terrorist (non-state actor but maybe state sponsored), nation state, foreign nation, economic competition, organized crime, foreign espionage, and basic script kiddies.

Next the types of attacks: social engineering, war dialer, dumpster diving, virus / worms, Trojan horse, imposter, denial of service, physical (power and connectivity), web page deface / vandalism, remote attack (modem) spoofing, installing back doors, logic bombs and electromagnetic pulse. The actual attack will be multidiscipline and use many online and actual techniques.

Finally the different objectives: damage to information: data destruction, manipulation, theft, or imitation, information warfare: web page defacements, loss of confidence in government, disinformation or media manipulation and disrupting the military or the governments ability to function.

Force protection factors can be looked at as counter IPB and will be issues the Army must deal with when conducting collection planning. They consist of using many of the following: policy of least privilege, security training, strong passwords, virtual private networks (VPN), public key infrastructure (PKI), pretty good privacy (PGP), encryption, biometrics, vulnerability scanners, snifers, auditing tools, backups, configuration management, deception tools (ie Honey Net), conducting risk assessment, reverse proxy servers for web based services, segmenting information and network resources, intrusion detection system (IDS), firewalls, anti-virus software. Security is a process (not a product) and requires defense-in-depth using a combination of tools to work.

Cyber space determining threat Courses Of Action (COAs) process:

- Identify the threat's likely objectives and desired end state.
- Identify the full set of COA's available to the threat. The most likely and most dangerous should be developed at a minimum.
- Develop COA's based on enemy perception of friendly information architecture (reverse cyber IPB).
- Evaluate and prioritize each enemy COA.
- Continue to refine COA's as time and new information allow.

These steps are the same in a conventional war or virtual war. The difference is where the battlefield is. Here is a brief scenario that shows what cyber IPB would have to include in its COA's during the wargaming process:

The day that would be called the electronic Pearl Harbor had many events. The president had just announced he would deploy forces to Taiwan. A FBCB2 command and control system in Korea was stolen. The Global Command and Control System's (GCCS) Time-Phased Force Deployment Data (TPFDD) database was compromised and modified. Out of work computer scientists from the Balkans were hired by a Middle East mineral rich third world country, relocated to Brazil, routed the attack through seven countries and gained access to New York Stock Exchange transaction records, changing 75% of the records. A worm targeted against 911 emergency center management

software was released. Two nuclear power plants in California had logic bombs in their mainframe database that caused meltdowns. Several military satellites were hacked into, damage unknown. The building housing Tier-One DNS servers were bombed, taking them off line for three days. China announced they had discovered a new vulnerability for router ACL updates and were releasing the patch. And finally a wave of web page defacements announced Taiwan was responsible for all the attacks.

The United States is in the best position to win on the digital battlefield, but the reverse is also true; the US is the most vulnerable country in the world to cyber attack. The speed of communications today not only means timeliness of information is key, but it is so fast we need to take the human out of the loop to stay inside the enemy's decision cycle. Another potential Digital Waterloo is when the United States declares war on a nation that had not been on the intelligence services radarscope previously. The country may have third world technical infrastructure but there are always pockets of high tech that the belligerents have access to. This means they may beat on drums to talk to the next village and then use a laptop hooked to a satellite phone to send encrypted email to someone on the next continent. These cyber guerrillas used bytes not bullets, by launching a disinformation campaign using international media and forced public opinion on their side.

Alternate Cyber space IPB doctrine

As the US Army transitions into the digital age it is imperative to determine how to port their analog doctrine or business processes into a digital doctrine that moves at the speed of the internet. The other option is to throw out the old process and start from scratch. To avoid the cycle of "preparing to fight the last war" the Army leadership needs to look at the current doctrine and see how it needs to be modified to be used in the cyber world

It is important to remember that hacking into systems is not IPB. Hacking is a method to gather information not a process to drive operational planning. It is important to note that senior commanders have been trained to receive information in a standard format and will need time to understand and take advantage of completely changing the intelligence portion of staff planning. This causes us to carefully consider the benefits of radical change. First lets look at a hack.

Anatomy of a hack: footprint (define target IP address, network location – basic prep for recon), scan (launch probe to determine actual machines and services – recon), enumeration (identify specific target vulnerabilities – create current situation map), gain access (launch actual intrusion – attack) [if the intrusion fails a denial-of-service attack can be launched with the information already gathered], escalate privilege (gain user account and upgrade it to administrator account – infiltrate), pilfer (steal info to get greater access –

intelligence collection cycle), cover tracks (edit auditing logs to erase evidence of all activity – provide cover and concealment), create back doors (access for next time – secure route). [xi]

These intrusion steps are great for gaining access but don't address staff planning needs. Next we need to analyze what intelligence collection needs to be done to support planning. Many techniques will be used to obtain the information but the first step is to start looking at the process that will support staff planning. Some initial steps are:

- Define the scope of the required information (not geographic area).
- Identify what is needed (holes in intelligence).
- Collection (using all types of cyber attack).
- Data management (collection, mining, processing).
- Artificial Intelligence correlation and filtering will be required due to amount of data that will be collected.
- Automated decision trees handling basic functions will increase speed.
- Graphic intelligence products displays will increase understanding.
- Point and click interface to collection management is objective process.

Bottom line:

IPB must be: timely, accurate, usable, complete, and relevant to be useful. In most cases the basic groundwork needs to be 80% complete before operations and logistics can start planning. This means cyberspace studies need to be developed now. The country studies of the cold war are obsolete as national boundaries disappear in the global information grid. Today commanders need network topology and information management studies.

Cyber IPB doctrine needs to be developed now and integrated into training installations and exercises to ensure leaders are ready to use it during the next conflict. No brand new development will be effectively used during the conflict. Tanks were developed during the First World War but the tactics to use them were not developed until afterwards and then effectively used in the Second World War. The Air Land Battle doctrine that won Desert Storm was integrated years before it was used allowing the leaders to understand and develop it to work for them. It needs to be part of rehearsals, simulation, testing and development now. Cyber IPB will also lead to cyber integration into other intelligent disciplines: Signals Intel (SIGINT), Electronic Intel (ELINT), Measurement and Signatures Intel (MASINT, Imagery Intel (IMINT), Human Intel (HUMINT), Open Source Intel (OSINT).

This article has addressed current, future and alternate IPB doctrine. As the US Army moves toward this information age revolution in military affairs it will have to conduct a paradigm transformation from the strategic to tactical level oriented on cyber space. It will need a new toolbox of capabilities that will allow

them to gain information dominance to fight and win on the future asymmetric battlefield. One of the first things that should change is the IPB process. It should be the first tool developed. To be effective it must be brought into the mainstream now to educate the leadership so they can fully integrate cyber IPB into the military decision making process when it comes time to fight and win on the new virtual battlefield.

---

[i] Kelley, Jack. "Terror groups hide behind Web encryption" USA TODAY February 2001. http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm

[ii] National Infrastructure Protection Center. "Cyber protests Related to the war on terrorism: The current threat" November 2001. http://www.nipc.gov/publications/nipcpub/cyberprotests1101.pdf

[iii] US Army. "FM 34-130 IPB" 8 July 1994 http://www.fas.org/irp/doddir/army/fm34-130/ch1.pdf

[iv] US Army. "FM 100-6 Information Operations" 27 August 1996 http://www.fas.org/irp/doddir/army/fm100-6/ch2.htm

[v] ibid.

[vi] ibid.

[vii] Major General Wang Pufeng. "The Challenge of Information Warfare" China Military Science, Beijing, Spring 1995. http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm

[viii] Office of the Secretary of Defense. "The Quadrennial Defense Review" 30 September 2001. http://www.comw.org/qdr/offdocs.html#nss

[ix] Joint Chiefs of Staff. "National Military Strategy" 1998. http://www.dtic.mil/jcs/nms

[x] Sun Tzu. "The Art of War" http://www.sonshi.com/sun-tzu_all.html

[xi] McClure, Stuart. Scambray, Joel. Kurtz George. "Hacking Exposed Third Edition" New York, 2001. McGraw-Hill

Last Updated: February 22nd, 2019

Upcoming SANS Penetration Testing

SANS Riyadh February 2019	Riyadh, Kingdom Of Saudi Arabia	Feb 23, 2019 - Feb 28, 2019	Live Event
Mentor Session - SEC504	Vancouver, BC	Feb 23, 2019 - Mar 23, 2019	Mentor
SANS Brussels February 2019	Brussels, Belgium	Feb 25, 2019 - Mar 02, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NV	Feb 25, 2019 - Mar 02, 2019	Live Event
SANS Baltimore Spring 2019	Baltimore, MD	Mar 02, 2019 - Mar 09, 2019	Live Event
Baltimore Spring 2019 - SEC560: Network Penetration Testing and Ethical Hacking	Baltimore, MD	Mar 04, 2019 - Mar 09, 2019	vLive
Baltimore Spring 2019 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Baltimore, MD	Mar 04, 2019 - Mar 09, 2019	vLive
SANS Secure India 2019	Bangalore, India	Mar 04, 2019 - Mar 09, 2019	Live Event
Mentor Session - SEC504	Dallas, TX	Mar 07, 2019 - Apr 25, 2019	Mentor
Mentor Session @Work - SEC504	Sao Paulo, Brazil	Mar 07, 2019 - Mar 13, 2019	Mentor
SANS London March 2019	London, United Kingdom	Mar 11, 2019 - Mar 16, 2019	Live Event
San Francisco Spring 2019 - SEC542: Web App Penetration Testing and Ethical Hacking	San Francisco, CA	Mar 11, 2019 - Mar 16, 2019	vLive
SANS St. Louis 2019	St. Louis, MO	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Singapore 2019	Singapore, Singapore	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS San Francisco Spring 2019	San Francisco, CA	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS vLive - SEC560: Network Penetration Testing and Ethical Hacking	SEC560 - 201903,	Mar 12, 2019 - Apr 18, 2019	vLive
Mentor Session @work - SEC504	Sao Paulo, Brazil	Mar 14, 2019 - Mar 21, 2019	Mentor
SANS Norfolk 2019	Norfolk, VA	Mar 18, 2019 - Mar 23, 2019	Live Event
Community SANS Chicago SEC504	Chicago, IL	Mar 18, 2019 - Mar 23, 2019	Community SANS
SANS Secure Canberra 2019	Canberra, Australia	Mar 18, 2019 - Mar 29, 2019	Live Event
SANS SEC504 Paris March 2019 (in French)	Paris, France	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Jeddah March 2019	Jeddah, Kingdom Of Saudi Arabia	Mar 23, 2019 - Mar 28, 2019	Live Event
Community SANS New Orleans SEC560	New Orleans, LA	Mar 25, 2019 - Mar 30, 2019	Community SANS
Community SANS New York SEC560	New York, NY	Mar 25, 2019 - Mar 30, 2019	Community SANS
SANS Madrid March 2019	Madrid, Spain	Mar 25, 2019 - Mar 30, 2019	Live Event
SANS SEC560 Paris March 2019 (in French)	Paris, France	Mar 25, 2019 - Mar 30, 2019	Live Event
Community SANS Toronto SEC542	Toronto, ON	Mar 25, 2019 - Mar 30, 2019	Community SANS
Community SANS Columbia SEC560	Columbia, MD	Mar 25, 2019 - Mar 30, 2019	Community SANS
Mentor Session - SEC560	Chantilly, VA	Mar 27, 2019 - May 29, 2019	Mentor
SANS 2019	Orlando, FL	Apr 01, 2019 - Apr 08, 2019	Live Event
SANS 2019 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Orlando, FL	Apr 01, 2019 - Apr 06, 2019	vLive