Document created: 2 November 99
Aerospace Power Chronicles - Contributor's Corner

What is Information Warfare?

Col Andrew Borden, USAF (Ret.)

Mind operates on sensations to create information for its own use. (Stan Franklin and Susan Oyama (1))

Phenomena become information through observation and analysis. (Cornerstones of Information Warfare. General Ronald Fogelman, USAF Chief of Staff and the Honorable Sheila E. Widnall, Secretary of the Air Force. 1997) (2)

Introduction

One result of the Information Revolution is a belief that warfare will be profoundly and permanently changed. The new warfare has variously been labeled "Cyberwar", "Information Warfare" , "Network Centric Warfare", "Information Operations" and "Command & Control Warfare" (C2W). Labels aside, nobody has presented an accurate model of what the new warfare will be. The result is that concepts, doctrine and definitions are lacking, so MOE' s cannot possibly be developed. Indeed, no quantifiable definition of the term "Information", itself, has been incorporated into any of the attempts toward IW modeling. This appears to be a fatal deficiency when the transition is attempted from abstract ideas to exercise and the battlefield, itself. A useful model must be based on consistent first principles and formal structured analysis. Then, the result can be shared, evaluated and used to support the development of war-fighting techniques in the Information Age.

Information Warfare Models

Two models of Information Warfare will be discussed in this paper: The USAF model described in the "Cornerstones of Information Warfare" (2) and the Network-Centric model developed by Vice Admiral Arthur Cebrowski (3). The Cornerstones was published in 1997 and signed by the (then) Air Force Chief of Staff and the Secretary of the Air Force. Admiral Cebrowski is the Director; Space, Information Warfare, Command and Control, CNO.

The following definition of IW is given in the Cornerstones:

> "Information Warfare is any action to Deny, Exploit, Corrupt or Destroy the enemy' s information and its functions; protecting ourselves against those actions and exploiting our own military information functions".

Without an operational (quantifiable) definition of Information, itself, this definition is not very useful. For example, how would you use this definition to assess performance in an IW exercise ? Perhaps we will be more successful if we examine the elements of IW and the specific means for execution of IW tasks and measures.

The quote above from the Cornerstones is reinforced by the Franklin/Oyama quote. Both suggest that "information" is never "out there" to be collected. Rather, we experience "Phenomena" or "Sensations" in the form of data and this *data* becomes information when processed in the presence of knowledge. This processing is characterized in (4). However, the Cornerstones document says that *information* is: collected, moved, stored and transformed. This is inconsistent with the quotation cited above from the same source. The document is also not clear about what *transformation* takes place and how it is accomplished. The Cornerstones also gives Information Attack measures as actions to:

Deny
Exploit
Corrupt or
Destroy

Enemy *information* and its functions. The means for accomplishing Information Attack are given as the following:

Operations Security (OPSEC)
Concealment, Cover and Deception (CCD)
Psychological Operations (PSYOPS)
Destruction (Hard Kill)
Electronic Warfare (EW)

These means have also been presented as the elements of C2 Warfare that is considered a subset (perhaps an exhaustive subset) of IW. (5)

It is difficult to find any logic or pattern in this set of elements. CCD can be considered a subset of OPSEC. At least they overlap substantially. Hard Kill applies to more military tasks than those in IW. PSYOPS is clearly an IW Attack Measure. EW is a very broad discipline, which overlaps substantially with OPSEC and CCD. This model cannot account for viruses that eat data files or operating systems (for example). It is very difficult to see how we could start with this paradigm and perform a structured analysis that would account for all of C2W or IW.

A second candidate model is the Network-Centric developed by Vice Admiral Arthur Cebrowski , a leading thinker in the realm of IW (3). Figure 1 shows the Network-Centric top level model. Not shown in the drawing is an Information Grid which encompasses all three elements, a Sensor Grid which encompasses the first two elements and an Engagement Grid which covers the last two elements. Several criticisms of this model are appropriate, most based on the "Apples and Oranges" principle. Sensors and Shooters are classes of objects. Command & Control is a very complex set of military functions. Moreover, sensors provide data...not information. To become information (reduce uncertainty) data must be processed in the presence of knowledge. (Data in the absence of knowledge is only noise). Moreover, it is difficult to imagine what "Information" would be provided directly to Sensors by Shooters. The only correct use of the term "Information" in this model is the data provided by Sensors directly to Shooters. Sensor positional data could match the Shooters Frame of Discernment and directly reduce his uncertainty about the location of the target.

An Operational Definition of Information Warfare

The fundamental idea is that *information* is not collected, stored, moved or used to reduce uncertainty. Information is *generated* in the course of reducing uncertainty so that decisions can be made. (4) In fact, information *is* the reduction in uncertainty measured in bits. This is consistent with the definitions of information and uncertainty given by Claude Shannon of the Bell Laboratories in the late 1940' s...definitions, which are now standard in the mathematical theory of information and communications (6).

Figure 2 is our view of the general problem addressed by IW. A decision-maker is presented with data from the world. He must use established knowledge to reduce his uncertainty about what this data means (perform Situation Assessment). When his uncertainty has been sufficiently reduced, he will be able to make a decision with confidence. An adversary may use IW Attack measures to interfere with the performance of IW tasks. Corresponding Protect Measures must be used to guarantee that the IW tasks can successfully be performed.

On the IW battlefield, there are only four tasks to be performed:

Data is:

Collected
Moved
Stored, and
Used to reduce uncertainty (perform Situation Assessment (SA))

In the process of Using data to perform Situation Assessment, Information is generated. The efficiency with which we can do this depends on the amount of data available (the information bandwidth) and the ambiguity in the data. This characterization (by the way) is a tantalizing analog of the Shannon-Hartley formula for the amount of information in bits that can be sent through a noisy communications channel with a specified bandwidth, the channel capacity:

$$C = W * (\log_2 (S/N)) \qquad \text{Formula 1}$$

Where W is the bandwidth and S/N is the signal to noise ratio. (Shannon)

If the efficiency of the Use of data can be measured by some analog of Formula 1, then the results of Attack and Protect Measures can be quantified. For example, if the use of concealment (an attack measure against the Collection task) reduces the efficiency of SA, than its effect can be stated in a way that is clearly understandable. The efficiency of SA is measured by determining the rate at which Information is generated in Bits per second. In later sections of this paper, it will be shown how the rate of Information production in the course of performing SA is measured.

There are only four types of Attack Measures possible against the four IW tasks. These are:

Degrade
Corrupt
Deny
Exploit

We prefer "Degrade" to "Destroy". Data can be degraded either by delaying it until its usefulness is reduced or by destroying it in full or part. For example, the use of concealment is an Attack measure (degradation) against the collection task. The use of jamming to reduce the Capacity of a communications channel (thereby delaying transmission) is another example.

To Corrupt is to insert false data. For example, the use of dummies on the battlefield is an Attack Measure against the Collection function. Intrusion into a communications channel and spoofing is another example. Psychological Operations (Psyops) is an example of Corrupting information being Stored in the protein processor (the human mind).

To Deny means to deny completely by a direct attack on the means of accomplishment. The use of a High Energy Laser to blind or destroy an electro-optic sensor is an example of denial by direct attack. Another example is a virus that destroys operating systems in a computer used to do Situation Assessment.

To Exploit is to Collect against the adversary' s Movement of Data. This increases the data available for friendly Situation Assessment and makes the generation of friendly Information more efficient.

The specific implementation of an Attack Measure depends on the means being used to perform the IW task. The specific implementation of a Protect Measure depends on the means being used to perform the IW task and the specific Attack Measure being used. For example, adaptive apertures are a Protect Measure against the High Energy Laser Attack Measure employed against an optical or E-O sensor.

If uncertainty is measured, an action is taken and uncertainty measured again...the difference in measurements corresponds to Information generated. The unit of measurement is in Bits. The ratio of Information to time is in Bits per second.

Since the key to measuring Information is to measure uncertainty repeatedly, it is important to understand the mathematical characterization of uncertainty. Uncertainty is always associated with a probability distribution: $\{p_i\}$ I = 1, 2, 3... where each $p_i >= 0$ and the p_i' s sum to 1. The formula for uncertainty follows:

$$H = -_i p_i * \log_2 p_i \qquad \text{Formula 2}$$

The minus sign is necessary because the log (base 2) of a number between zero and 1 is negative. This formula is illustrated by the following example.

In the mind of Paul Revere, land and sea attacks were equi-probable. That is, Probability (Land) = Probability (Sea) = 1/2. A lookout in a nearby tower was to observe the approach of the British Forces and encode the information about the method of approach as follows:

> Show one lantern if by land, two if by sea.

Since $\log_2 (1/2) = -1$, computation using Formula 1 shows that Paul Revere had one bit of uncertainty. History tells us that Paul Revere saw two lanterns (data). He applied his knowledge of the code given above to deduce that the British were approaching by sea. His uncertainty had been reduced to zero. This intuitive situation is confirmed again by formula 1 with the Probability (Land) = 0 and the Probability (Sea) = 1. (If we define $0*\log_2 0 = \text{Lim}(x$) (1/x)*log (1/x) which equals 0). We conclude that Paul Revere received one bit of Information because his uncertainty had been reduced by one bit. This is consistent with the Shannon definition of uncertainty.

Reference (4) contains a detailed discussion of how data becomes information. Briefly, an active memory compares data with a static data base. The active memory and the data base taken together, function as an associative memory, adjusting the values in a nearness function or metric to reduce the uncertainty about the meaning of the data.

In this case, Paul Revere had the benefit of a noiseless communications channel and unambiguous decoding of the message. In IW, we rarely have an ideal situation like this. There is usually a great deal of ambiguity, which the decision-maker has to deal with. In situations with a great deal of ambiguity, it is a great challenge to develop a strategy for decision-making, which produces on-time, high confidence decisions.

THE EFFICIENCY OF DECISION-MAKING

IW is all about measures to improve (or degrade) the efficiency of decision-making. The maximum theoretical efficiency depends on the amount and quality of data available and on the amount of ambiguity in the data. The achievable efficiency depends also on the strategy used to generate information from data. If we had an ideal or canonical strategy to generate information, we could measure the value of any IW measure applied to data by considering the change in efficiency, which results from its application. For example, if the introduction of a dummy radar transmitter introduces ambiguity into the radar parametric data base, we would wish to measure the effect on our ability to identify and classify radars in seconds or in bits of information generated per second. For another example, if the adversary introduces a low probability of intercept (LPI) communications system, he degrades our ability to determine the amount of traffic on the link, thereby reducing the amount of data we have available to generate information and make decisions. The reduction in efficiency would be a good measure of the effectiveness of the LPI IW measure. This method is our roadmap to developing MOE' s for IW.

The task of determining the theoretical efficiency of information generation (uncertainty reduction) is not easy. To do this, we need a canonical or standard method for designing decision-making systems. This method must guaranty that it always designs a nearly optimal system. This nearly optimal system will be the baseline for measuring changes in efficiency which result from attack (or protect) IW measures.

The difficulty of designing good decision-making strategies comes from two facts:

> Each source of data has a different cost, usually in time. For example, radar parameters at the pulse level are very easy to obtain. Parameters concerned with scan characteristics require a long observation time and are expensive to determine.
>
> Each source of data makes a different information contribution (has a different amount of ambiguity) and this depends on the current state of the problem, i.e. which other data elements have already been consulted.

Taking these two facts into account means that we must consider the contribution of data to the timely solution of the problem. The units for this contribution are bits per second. Computing the bits per second of information to be derived from a data source requires heavy computation involving many conditional probabilities. That' s what computers are for.

The result of this design method is a nearly-optimal, standard strategy for making decisions (doing Situation Assessment). One of the positive results of having to do so much computation is that a report card for the SA strategy can be produced. The report card can provide statistics on throughput and confidence in any form required by the designer/user, making informed go/no-go decisions possible.

One of the elements in the report card is the number of decision-tree nodes that have to be produced to give a result meeting operational requirements, if they can be met at all. This statistic has two important implications. The first is that, if requirements cannot be met with any number of decision tree nodes, there is a need for additional Information bandwidth more data. This immediate feedback on the adequacy of the SA strategy is operationally very important.

The second implication was a surprising result of several experiments done in the area of Indications and Warning (I&W). We found that *a priori* assessment of the difficulty of a specific I&W task was very unreliable. Two very similar-looking tasks were found to differ by two orders of magnitude in difficulty, measured by the numbers of decision-tree nodes that had to be generated. With so little intuition into the nature of the task, it would be very difficult to build efficient I&W strategies by any method, which depends on human insight.

Conclusion

This paper contains a critique of existing models of Information Warfare and a sketch of a better model one which is operational in the sense that its elements can be quantified. This model has potential to be used in the planning, execution and evaluation of IW exercises and in the development of IW doctrine and tactics.

Notes

1. Franklin, Stan, Artificial Minds, Cambridge, MA.: The MIT Press, 1995 Oyama, Susan, The Ontogeny of Information, Cambridge, MA, Cambridge University Press, 1995.
2. The Honorable Secretary of the Air Force, Sheila E. Widnall and General Ronald R. Fogelman, USAF Chief of Staff, Cornerstones of Information Warfare, 1997.
3. Silverberg, David. (Editor), Network Centric Warrior, Q&A. Interview with Vice Admiral Arthur Cebrowski, Director Space, Information Warfare, Command and Control, Chief of Naval Operations. M Information Technology, April-May 1998, Volume 2, Issue 2.
4. Col. Alan D. Campen, USAF (Ret.), "Rush to Information-Based Warfare Gambles with National Security, Signal Magazine, July 1995. Pages 67 69. Signal is the official publication of the Armed For Communications and Electronics Association (AFCEA).
5. Col. Andrew Borden, USAF (Ret.) "The Design and Evaluation of Situation Assessment Strategies", Information and Security, An International Journal, Volume 1, Number 1, Summer 1998.
6. Shannon, C.E., " A Mathematical Theory of Communications", Bell Syst. Tech. J. 27, (1948) 379 423 and 623 656.

Contributor

Andrew Borden is a mathematician with long experience in Electronic Warfare. He has published many papers on the subject of decision-making systems. Mr. Borden is a retired Air Force Officer. His last active assignment was as Deputy Chief of Staff for Intelligence in what is now the USAF Air Intelligence Agency. He has advanced degrees in mathematics from the Kansas State and Ohio State Universities. Currently associated with DRH Consulting, San Antonio, TX. The address for correspondence is: 1210 Scenic Knoll, San Antonio, TX 78258. Email: borden@wireweb.net or borden@zajil.net

Disclaimer
