CORDA

Attack of Trust

Paper for Twenty-second International Symposium on Military Operational Research (22 ISMOR)

by Rowland Charles Goodman

September 2005

CRDDPD 009 002/TN.3

The views contained herein are those of the author or of the authors being quoted, and are not to be construed as reflecting the views of CORDA or BAE Systems.

CORDA

Brennan House, Farnborough Aerospace Centre, Farnborough, Hants, GU14 6YU

Telephone: 01252 383238 Facsimile: 01252 383544

.

Summary

This paper is based on work carried out by CORDA in 2004 on the attack of trust. Our client was the Future Systems Division of BAE Systems.

The attack of trust is part of the psychological aspect of two modern concepts of operation: 'Effects Based Operations' (EBO) and 'Shock and Awe'. EBO is the current intellectual framework for at least Air Force operations. 'Shock and Awe' was employed in Iraq in 2003. It seems likely that EBO will be an important part of the future tri-service defence context.

In order to do Effects Based Operations, one needs to be able to assess both primary and nth-order effects. This is required both to justify investment, and to conduct Effects Based Operations.

As a starting point, CORDA undertook a study of the attack of trust, which is an element of the overall problem.

Aims and Objectives

The aims of the study were as follows:

- To develop an understanding of existing work on the theory and practice of measures of performance and measures of effectiveness, in the context of EBO and IW, particularly regarding trust.
- To develop a qualitative model of Trust attack, in the form of a set of influence diagrams showing the structure of the attack process and its links to the wider context in which the system being attacked is used and the attack has its ultimate effects. (These influence diagrams are in the full report, though not in this paper.)

This Paper

This paper contains the following:

- A description and explanation of the domains of trust. (Section 2.)
- Practical applications of trust and attack of trust in a military context, including why some national armed forces have greater problems than ourselves. (Section 3.)
- Measures of Effectiveness (MoEs) for eight different forms of trust attack against command and control. Note that MoEs for effects based operations are different from those that people use for attrition-based warfare. (Section 4.)

The Full Report

The full report also contains a literature survey, and influence diagrams for trust attack.

Approvals

Signature		
Author	Rowland Charles Goodman	August 2005
Signature		
Approver	Dominic Heritage	August 2005
Signature		
Authoriser	Noel Corrigan	August 2005

Contents

1 Introduction

Trust is an essential part of human relationships. Without trust one cannot form relationships such as friendship or marriage, and it is difficult to work with people. People also need trust in the tools they use. Trust is also important in advanced telecommunication systems such as those used by credit card companies and the internet. There one has a complex web of trust: trust between different computer systems, trust in information, and trust between people and these systems.

Like all other human relationships, military command systems have always involved trust. The trend is to use internet protocols (or similar) for some parts of modern command systems. Trust is therefore complex.

In 2004, CORDA undertook a study of the 'attack of trust' in a command and control context for the Future Systems Division of BAE Systems. This study forms part of a wider set of studies of Effects Based Operations (EBO). The study has included

- A literature survey (not included in this paper)
- Talking to various people in BAE Systems about work that they know of.
- Discussion of trust in a broader military context (Section 3).
- Development of Measures of Effectiveness (MoEs) for trust attack. Note that effects based MoEs are different from attrition-based MoEs (Section 4).
- Development of qualitative modelling of trust attack (not included in this paper).

The study was documented in a full report.[1] This paper contains the results of some of the thinking, which went into the study.

[1] "Attack of Trust, Literature Survey & Qualitative Modelling", by RC Goodman, CORDA Report CRDDPD 009 002/TN.2, September 2004.

1.1 Objectives of the Original Study

The objective of studying the attack of trust was to initiate development of methods of assessing the benefits of trust attack, and as a first step in developing assessment methods for Information Operations in general.

The problem with assessing Information Operations is that their results are less obviously tangible than assessing physical effects (such as weapons that destroy bridges). Nevertheless information operations are, and have always been important. For instance, a German estimate of the effectiveness of successful British information operations against U-boats in the second half of 1941, was that they reduced British merchant ship losses by 69%.[1]

1.2 Definitions of Trust

"We do not have in cognitive and social sciences a shared or dominant, and clear and convincing notion of trust. Every author working on trust provides his/her own definition, frequently not really general but aimed at being appropriated for the specific domain (commerce, politics, technology, etc.)."[2]

1.2.1. What is Trust?

Trust can be defined as a "firm conviction in another's reliability, integrity, honour; implicit confidence, faith, reliance". The phrase 'to take something on trust' means "to believe that it is what it appears or is asserted to be, without looking closely into the evidence for oneself."[3]

An important point about trust is that if one has complete trust, one does not need verification.

---

[1] During second half of 1941, Britain was reading the German codes for U-boats (Enigma). The information gained was used to route convoys away from U-boat patrol lines, to concentrate escorts on threatened convoys (by taking them away from those that were no longer threatened), and to attack German logistics. The British also tried to ensure that the Germans continued to trust Enigma. Pages 367-8 "Germany and the Second World War, Volume VI", by Horst Boog, et al, pub in English by Clarendon Press, 2001.

[2] T3 Group. (T3 = Trust Theory Technology.) T3 Group is a research team founded in 2003, in the Institute of Cognitive Sciences and Technologies (ISTC) at the National Research Council (CNR), in Rome, Italy. http://www.istc.cnr.it/T3/trust/

[3] "The Universal Dictionary of the English Language", edited by Henry Cecil Wyld, pub Waverly, 1st edition 1932, 8th impression 1956.

Trust is an abstract concept. It is not a stock, or a flow; and it cannot be directly measured. Nevertheless, people would like to measure either trust or the degree to which they should trust.[1]

There are different domains of trust (and different meanings of the term domain). These are discussed in Section 2.

1.2.2. What Are Distrust and Mistrust?

The following definitions may be useful (though they are not universally accepted):[2]

- '**Distrust**' where one did not trust, and was right to not to trust.
- '**Provisional distrust**' where one felt one ought to check before trusting. It should be recognised that people sometimes check even though they are minded to trust (for all sorts of reasons), and that experiments on trust would categorise such behaviour as showing either 'distrust' or 'provisional distrust'
- '**Mistrust**' where one did trust, and was wrong to trust. (In the author's opinion, this use of 'mistrust' is unwise, as it will generally be misunderstood. In Standard English 'mistrust' and 'distrust' are essentially the same.[3])

'Distrust' is sometimes used to mean all three. It is worth noting that distrust is not necessarily bad – for instance distrusting a system that does not work correctly.

1.2.3. What Can Trust Exist Between?

Trust can exist between:

- People and other people, both on an individual basis, and in the context of an organisation.

---

[1] Section 1.2 mentions that work that the ATC at Filton hopes to do for the US DoD will involve experimental measuring of trust. Section 2.2 discusses the concepts of 'guaranteed' and 'actuarial' trust, which describe methods of assessing whether to trust.

[2] Pages 14-15, "Trust, Mistrust and Distrust of Information", by Barry McGuinness, Jan 2004. Minutes of meeting with Barry McGuiness 29 July 2004.

[3] "The Universal Dictionary of the English Language" defines distrust and mistrust as follows:

Distrust (noun) "Want of confidence; doubt, suspicion." (verb) "To feel distrust concerning, lack of confidence in, be suspicious of."

Mistrust (verb) "To have no trust or confidence in; to suspect, doubt." (noun) "Suspicion, distrust, want of confidence."

- People and information. Note that this is 'one-way'; people may trust information.

- People and machines. People often relate to some machines as if they were people. Even when they do not, the issue of whether one trusts one's radar warning receiver is important. One might decide to ignore the data it produces, or even to switch it off for fear that it might attract enemy aircraft.

- Machines and other machines. Trust relationships between computer systems are important, both in the military sphere, and in commercial organisations such as Google, internet retailers, and credit card companies. In some cases such computer systems exhibit similar behaviours to human organisations grappling with similar problems (for example in maintaining trust in message delivery). Not everyone accepts that inter-machine trust should be regarded as 'trust'.

In the context of a modern or future network-centric command system, all four types of trust may be inter-mingled because the command system will be a mixture of human and machine systems.

1.2.4. What is Trust Attack?

A successful attack of trust can be defined as achieving one or more the following:

- "I don't trust true information.
- I trust false information.
- I need more time to decide.
- I don't trust the system and won't use it."

This definition is too narrow. An examination of historical examples shows that it is possible to successfully attack trust by exposing lies and making people believe in the truth.[1]

When discussing attack of trust it is possible to become tied up in semantics. For instance, if one digs craters at an airfield, one may fool enemy battle damage assessment into thinking that the airfield has been knocked out. This is an attack on trust by the above definition. One is making the enemy trust that he has knocked out the airfield.

[1] The obvious example is the 1956 Suez Crisis, where the British Government made false claims, which were widely disbelieved. The loss of trust led to the Government abandoning Operation MUSKETEER.

1.3 Validation

Some form of validation is desirable for any new concepts and for modelling. In this study, we have tried to achieve a limited validation by asking if a type of operation or attack of trust has happened in the past.

2 Domains of Trust

The term 'domain' is frequently used with respect of trust. However there are different schemes, with different definitions.

- 'Domain' can mean the setting or context for trust ('interpersonal', 'organisational', 'online', 'automation', and 'information trust'). This seems to be the most common use. (See Section 2.1.)

- 'Domain' can also relate to the reason for trust ('actuarial' and 'guaranteed' trust). (See Section 2.2.)

- 'Domain' is also used to mean a high level grouping of network entities (e.g. on the internet or Windows NT). [1] Since trust is required within such groupings, literature on this subject also talks about 'domains of trust'.[2] In the IT sense, a 'domain of trust' can be an area in which trust exists (in UNIX each user has his own domain), or even a trust policy.[3]

---

[1] "SIP security requirements from 3G wireless networks", by D. Kroeselberg, January 2001.
http://www.softarmor.com/wgdb/docs/draft-kroeselberg-sip-3g-security-req-00.txt

[2] "The role of a firewall is to stratify a network infrastructure into domains of trust, by delineating zones, and regulating communication between them. The behaviour of a firewall should be a representation of the security policy, which it supports." "Securing Your Network: Protecting Valuable Corporate and Intellectual Property in an e-nabled World", by Ajay K. Sood, Nokia Internet Communications, Toronto, Canada.
http://www.ewh.ieee.org/reg/7/canrev/canrev39/sood.pdf

[3] "Several domains of trust should be considered:
- trust nobody.
- trust the government.
- trust everyone on the machine—everyone that has an account on the machine is trustworthy.
- trust the administrator(s) on the machine.
- trust everyone on a local network.
- trust the administrator(s) for the network of machines.
- trust everyone on a wide area network or an inter-network (such as the Internet). One has to be incredibly naïve to have this much trust)."

"Security: System Protection", by Paul Krzyzanowski, Rutgers University, 1997-9.
http://www.pk.org/rutgers/notes/pdf/11-security.pdf

'Domain' also has a human factors meaning. In this case we are not talking about 'domains of trust', but domains that affect the decision to trust.[1]

- *Information domain*. Information available to the decision-maker.
- *Cognitive domain*. The thoughts of the decision-maker.
- *Social domain*. Interactions with other people that affect the decision-maker (i.e. social pressures, organisational factors, etc.).
- *Physical domain*. The effect of the physical environment on the decision-maker.

2.1 Domain as a Setting or Context for Trust

The usual sense of 'domain' is as a setting or context for trust. This is the sense used in "Trust, Mistrust and Distrust of Information", by Barry McGuinness.[2] This has five domains of trust:

- *Interpersonal trust*. Trust between individuals: the extent to which a person is confident in, and willing to act on the basis of, the words, actions, and decisions of another.
- *Organisational trust*. This is also known as 'social trust'. This is the effect of an organisational setting on interpersonal trust. Because one knows that an organisation has values, aspirations, rules, procedures, accountability, checks and balances, etc. one may trust the organisation. (A good example of this is that I am happy to give money to a person I have never seen before, simply because he/she is working behind a till at my bank.)

---

[1] Other social sciences, which deal with trust have their own definitions of domain. For instance there are the 'three domains of education', which were devised by Benjamin Bloom between 1948 and 1956 and are widely used:

"*Cognitive Domain*. What people know and how they think about what they know.
Affective Domain. What people feel and how intensely they hold these feelings.
Psychomotor Domain. What people can do and how skilful they are in doing them."

"Risk Communication: The Educators' Perspective", pub SEE Biotech, University of Wisconsin-Madison. http://www.biotech.wisc.edu/seebiotech/powerpoints/n2002douglah.ppt

"Learning Domains or Bloom's Taxonomy". http://www.nwlink.com/~donclark/hrd/bloom.html

[2] "Trust, Mistrust and Distrust of Information, White Paper for Evidence Based Research Inc, on behalf of the Office of the Assistant Secretary of Defence for Networks and Information Integration (OASD/NII)", by Barry McGuinness, BAE Systems Advanced Technology Centre, JS15203, Jan 2004.

- *Online trust*. This has three meanings:
  - Interpersonal or organisational trust via an electronic network (such as the internet or the telephone system).
  - Trust in online commercial entities, their web-sites, and products.
  - Trust in the technology itself.

- *Automation trust*. Trust in equipment to perform as expected. Many people exhibit trust behaviour towards equipment such as computers and autopilots that strongly resembles interpersonal trust. The most important difference is that the behaviour is not reciprocal. This seems to be the main difference between automation trust and online trust - online trust can be reciprocal.

- *Information trust*. Trust in the authenticity, validity, and reliability of information received or accessed.

These domains are not necessarily exclusive. There can be conflicts between domains. For instance one may deal with trusted people from untrustworthy organisations, or one might believe that a piece of information from a trustworthy source was wrong.

2.2 Domain as a Reason for Trust

Another scheme (or partial scheme) of domains of trust has been encountered with respect of commercial transactions in which 'domain' relates to the reason for trust:[1]

- *Actuarial Trust*. "Life insurance companies can trust they will have a certain investment horizon for your policy, based on actuarial tables. The life insurance company does not get your pastor, your mother, or your banker to guarantee you will live to a certain age. The insurance company, sadly to say, is not even very concerned what age you live to, except as it may affect their actuarial averages. A major grocery chain is willing to accept checks from strangers because the actuarial experience of grocers has shown that less than one half of 1 percent of those checks will go bad. Obviously life insurance companies and grocery stores will try to tweak the odds: with life insurance companies accepting only non-smokers or grocery stores rejecting checks with low check numbers. But fundamentally, the trust comes from actuarial dynamics, not from some external guarantor."

---

[1] "The Future of Money in the Information Age", Chapter 3, "Electronic Liquidity and Domains of Trust", by William Melton, pub CATO Institute. First presented at the Cato Institute's 14th annual Monetary Conference, "The Future of Money in the Information Age", which was held in Washington, D.C., on May 23, 1996.
http://www.cato.org/pubs/books/money/money3.htm
http://www.cato.org/pubs/policy_report/v18n4-6.html

- *Guaranteed Trust.* "The second type of trust domain is one that we are more familiar with: the domain of guaranteed trust. In this type of domain, the government, the bank, or some other strong guarantor says, 'Trust me, I guarantee it.' Behind any guarantor there may be another guarantor, such as behind your bank stands the Federal Deposit Insurance Corporation, and behind the FDIC is the perceived strength of the government. Thus, these guaranteed trust domains quickly become very hierarchical."

"Frequently, there is a mixing of actuarial and guaranteed trust domains. For example, though you as employer may not personally know all of your 500 employees, you believe you have followed good hiring practices and therefore you can say to your bank: 'Please extend to my employees liquidity for travel expenses, and I will make good if anyone fails to pay.' You have made the actuarial assessment of trust internally, then converted that into a guaranteed trust in dealing with the bank. The bank does not have a clue about your employees; it is looking to your guarantee for its trust.

"The distinction between liquidity based on actuarial analysis and on a guarantor relation, although subtle, has substantial social, political, and economic implications. The actuarial domain of trust is frequently found in a market economy, while the guaranteed domain of trust is more at home in hierarchical environments. Modern financial markets spring from the sharing of risk and are actuarial by nature. Even the largest guarantors (governments) are subject to the statistical evaluations of those markets or actuarial domains. As a national and international economy, the United States is moving, and must move, toward actuarial domains of trust."

When credit cards got started, they were heavily dependent of guaranteed trust provided by local and merchant banks, linked up using then-advanced telecommunication systems. System risks were managed using actuarial trust. As credit card systems have evolved, they have reduced their dependence on guaranteed trust, in favour of greater actuarial trust. Part of the reason for the change is that actuarial trust is cheaper to administer than paying for guarantees from banks.

The internet makes heavy use of guaranteed trust, both in the form of certificates (a largely-invisible internal working device), and the use of credit cards to verify both the ability to pay, and that users are 18 or over.

The Wisdom of Crowds. There are some interesting bases of trust used by a number of web-sites, whose intellectual underpinning can be described as 'the wisdom of crowds'. Where large numbers of informed people make

independent judgements, the average of their judgements may be better than that of individual experts.[1]

- EBAY exploits this principle with its feedback principle of establishing trust. Both vendors and customers leave feedback at the conclusion of each transaction. This enables other users of EBAY to assess the trustworthiness of the people they deal with. [This method is backed up by a guarantee by EBAY ('guaranteed trust'), and by rules and procedures ('organisational trust').]

- Search engines such as Google use the number of references to a web-site to establish trust in it. The more independent references, the greater the trust, and therefore the higher the reference appears on the list. [There are, of course, other considerations such as relevance.]

These 'wisdom of crowds' methods are a combination of actuarial and guaranteed trust. The individuals who make the references or leave feedback, are providing a form of guarantee, which is assessed quasi-actuarially.

[1] "The Wisdom of Crowds; Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations", by James Surowiecki, pub Doubleday, 2004. http://www.randomhouse.com/features/wisdomofcrowds/

3 Military Applications of Trust

The purpose of this section is to describe some of the military applications of trust. Some historical examples have been given to help give a better understanding. Applications of trust include

- Trust within a small unit (Section 3.1)
- Automation trust (Section 3.2)
- Trust in the context of command and control (Section 3.3)
- Political trust (Section 3.4)

Trust reduces the need for verification, and it is an enabler. In military situations where trust is low, tactics and operating procedures will be modified accordingly (alternatively they will not work).[1]

---

[1] Whilst is easy to demonstrate that tactics and procedures do not work that well if trust is low (see Section 3.1), it is not so easy to prove that military organisations modify their methods of operation to cope with low trust. However there are some historical examples:

At various times armies have had problems with individual soldiers deserting their posts, or slipping away when their unit was attacking. The Soviet Army at times during World War II, and the German armed forces in 1945 reportedly used on the spot execution of such people.

The 'line of battle' used by Western European navies in the 18th Century was introduced in the 17th Century because of lack of trust in both individual ship captains and subordinate admirals. The advantage of the 'line of battle' formation was that it allowed verification of whether a commander was doing his duty, whereas the previous styles of battle did not. There were many disadvantages in this style of fighting: it was difficult to bring on a battle, and it tended to be indecisive. However the verification issue was more important. At the Battle of Trafalgar in 1805, the combined French and Spanish fleet had their ships deliberately intermingled to enhance trust. (i.e. If they had been separate, then one ally might have deserted the other.) Nelson was willing to risk a pell-mell battle, and thereby achieve a decisive result, because of the high (and atypical) degree of trust between the captains of his fleet (which is why they are sometimes described as a 'band of brothers').
"Naval Warfare in the Age of Sail, the Evolution of Fighting Tactics 1650-1815", by Brian Tunstall, pub Conways, 1990.

3.1 Trust Within the Small Unit

Military units are composed of a hierarchy. It helps to understand how trust can work inside a small team. This section will consider trust within the following examples:

- A gun team (Section 3.1.1).
- An infantry section (Section 3.1.2).
- A battalion (Section 3.1.3).
- What happens if the trust relationships are damaged (Section 3.1.4).
- Why some armed forces do not develop such good trust relationships (Section 3.1.5).
- How armed forces with a weakness in this respect can try to compensate (Section 3.1.6).

3.1.1. Trust within a Gun-Team

A good simple example of trust within a small team is a gun team for a manually loaded artillery piece.[1]

Even as late as the 1980s, well-trained gun teams in the Royal Navy could make as good a rate of fire with a manually loaded 4.5" gun as an automatic gun on board ship. This was achieved by practice so that the team could work together almost automatically. This developed a form of trust; each member of the team could trust the other members of the team to be where he thought they would be. This is particularly useful when passing ammunition. If you have to look to see that the next person in the chain is ready, before you do your part, then the rate of work is much slower.

A key element in building trust was practising the team together (i.e. collective training). If you put new people in the team, then the new people would have to practise in the team to become fully integrated with them. Having standard drills (i.e. ways of doing things) made it easier and quicker to train people together, and to train replacement members of the team.

(Of course this is not the only element that makes a difference. Good ergonomic design can make a factor of 10 difference in the rate of fire.)

[1] Whilst manually-loaded artillery is becoming a thing of the past in navies; most armies still use manual-loading artillery.

3.1.2. Trust within an Infantry Section

Whilst the operations of men in an infantry section are not quite as integrated as those in a gun-team, they are still mutually dependent. In battle men fight for their mates. [1] They know that if they hide and do not take part, they are letting their mates down – their mates may get killed because of this.

In the infantry section there are two sorts of mutually reinforcing interpersonal trust:

- Trust between mates, built up through bonds of friendship and living together (for a least some of the time).
- Trust in each other's abilities, built up by both individual and collective training.[2]

It is also important that people trust that if they get hurt, they will be looked after, and that their families will be looked after.

An important role of the organisation is to foster these kinds of trust.

3.1.3. Trust with a Battalion

The battalion consists of a hierarchy in which sections are one of the smaller building blocks. Clearly it is not possible in a battalion of roughly 800 men, for everyone to be 'mates' with everyone else. If the battalion merely depended on the command hierarchy, it would be quite weak. However battalions also have institutions to build strong cross-links between leaders on the same level, such as sergeants' messes and officers' messes. Collective training also helps. The command network enables the

---

[1] "I hold it to be one of the simplest truths of war that the thing which enables an infantry soldier to keep going with his weapons is the near presence or the presumed presence of a comrade. The warmth which derives from human companionship is as essential to his employment of the arms with which he fights as is the finger with which he pulls a trigger or the eye with which he aligns his sights. The other man may be almost beyond hailing or seeing distance, but he must be there somewhere within a man's consciousness or the onset of demoralization is almost immediate and very quickly the mind begins to despair or turns to thought of escape." Page 42, "Men Against Fire", by S.L.A. Marshall, pub Morrow, 1947.

[2] "Trust in Small Military Teams", by Barbara D Adams and Robert DG Webb, Humansystems Incorporated, presented at 7th International Command and Control Research and Technology Symposium, 2002. http://www.dodccrp.org/events/2002/7th_ICCRTS/Tracks/Track_3.htm. Copies of pdf file of this paper are named "006.pdf" and "[CCRTS] Trust in small military teams.pdf".

This is an interesting paper, which expresses things known about for at least the last hundred years, in terms of modern trust jargon as if it were all new stuff. It focuses too much on the appreciation of comrades' technical and tactical skills, and does not take sufficient account of the 'mates' aspect of trust in this situation.

dissemination of knowledge that can also help to build trust. Thus, though all these measures there can be strong interpersonal trust across the battalion. As with the section, this trust benefits from both friendship and professional appreciation.

The battalion also benefits from organisational trust: i.e. people knowing what is expected of them, and what to expect of others. This organisational trust has both checks and balances, rewards and punishments.

At battalion level, the unit also has the kinds of command and control trust relationships described in Section 3.3.

3.1.4. What Happens if the Trust Relationships Are Damaged

Introducing new people into the organisation can temporarily weaken it.[1] There are three potential reasons for this, one of which is interpersonal trust:

- People will need time to build up interpersonal trust relationships with the new people.
- The new people may be less well prepared for combat. For instance they may be reservists. They may be less fit. They may need individual and collective training.
- In armed forces that lack common doctrines and standard ways of doing things,[2] either the new people will have to learn the way of doing things in the organisation they have joined, or (and this can happen with a new commanding officer) the rest of the organisation may have to adapt to new ways. Either of these can cause both interpersonal problems and issues of organisational trust.

Peacetime units frequently need to be brought up to wartime establishment before they can be deployed on operations. One method that has been

---

[1] Page 86, Vol I "On War of To-Day", Friedrich von Bernhardi, trans Karl von Donat, pub Hugh Rees, 1912.

David Rowland has produced an empirical relationship from historical data on the effect of a battalion's experience of combat on the number of casualties it will suffer in similar engagements. The more experienced the unit, the fewer casualties it will suffer. In this relationship, the effect of providing replacement personnel is to diminish the benefit the unit gains from prior experience. This work was initiated when David Rowland was a scientist at DOAE West Byfleet, and continued at DERA, and DSTL. "A Compendium of Information For Modellers and OA Practitioners Derived From Historical Analysis", by Paul Glover, Rowland Charles Goodman, and Michael J Young, Dstl Report Dstl/TR14025 V1.0, March 2005.

[2] Historically, the British armed forces have tended not to have common doctrines and standard ways of doing things.

used by the British Army is to bring in whole sub-units (companies/squadrons) to bring a battalion/regiment up to strength. That way the interpersonal relationships up to company/squadron commander are maintained. Another solution is to spend a great deal of time on collective training before the start of the fighting. Both these solutions were done, for example, during Operation GRANBY in 1990-91.

In wartime, battle casualty replacements need to be introduced carefully and allowed time to 'bed in'.[1]

A well-documented example of how this can go wrong is that of 6th Battalion Duke of Wellington's Regiment (6 DWR) in Normandy in June 1944. The battalion first saw combat on 13th June 1944. During the next two weeks they took heavy casualties (23 officers and 350 other ranks by the end of the month).[2] They received replacement personnel, who were put into the unit as individuals at a time when the battalion was in the front line area and was taking casualties most days. There was a breakdown of trust within the battalion. By late June the other ranks often ran away during action – newly posted officers got themselves killed trying to stop this. Finally a replacement battalion commander had the courage to write a report saying that the battalion should either be taken out of the line and retrained, or it should be disbanded.[3] The battalion returned to England in early July, and disbanded in late summer.[4]

---

[1] "It has happened too frequently in our Army [the US Army] that a line company was careless in the manner in which it received a new replacement. The stranger was not introduced to his superiors nor was there time for him to feel the friendly interest of his immediate associates before he was ordered forward with the attack. The result was the man's total failure in battle and his return to the rear as a mental case." Page 42, "Men Against Fire", by S.L.A. Marshall, pub Morrow, 1947. See also "Cohesion and Disintegration in the Wehrmacht in World War II", by Edward Shils and Morris Janowitz, 1948,

An apparently contrary view is taken in "Hell in Hurtgen Forest: the Ordeal and Triumph of an American Infantry Regiment", by Robert S.R. Lawrence, pub Kansas University Press, 2001. A review of the latter on pages 203-4 of the Spring 2003 issue of "Parameters" criticises RSR Lawrence for trying to make too much of limited information.

[2] In part because they did stupid things like having a battalion meeting in ground over-looked by the Germans. War Diary 6 DWR, June 1944, currently stored at PRO Reference WO166/15096.

[The author remembers that ten years ago the 1944 war diaries for 6 DWR up to June had a WO172 reference, whilst the ones from July onwards had a WO166 reference. This war diary appears to have been re-catalogued.]

[3] "Report on State of 6th DWR, 49th Div", 30 June 1944. PRO Reference WO205/5G, and WO166/15096. Exerts are quoted on pages 282-3 of "Decision in Normandy", by Carlo D'Este, pub Harper, 1983.

[4] Note that page 283 of "Decision in Normandy", by Carlo D'Este, is incorrect in stating that it had been disbanded by 6th July. See WO166/15096.

The US Army in Vietnam had policies on soldiers' tours of duty, which damaged trust within the unit. Battalion commanders had a tour of duty of 6 months, company commanders 3 months, whilst enlisted men had a tour of 12 months. Personnel were rotated in and out of units as individuals. "The constant rotation of officers and men in and out of Vietnam bred units of what were essentially strangers, men unfamiliar with and often distrustful of their comrades in arms… The set tours also engendered a preoccupation with surviving until the date of departure".[1]

3.1.5. Why Some Armed Forces Do Not Develop Good Trust Relationships

The following was written in 1975 to explain some of the reasons why Arab armies performed poorly in the Arab-Israeli wars.[2] It gives a good description of what sort of trusting behaviour is needed in an infantry unit, and deficiencies in Arab armies.[3]

"In 1967, as in later years, differences in technical skill between Arabs and Jews have been much less significant than differences in social conduct.

"From the pair of infantrymen who advance in tandem, where one runs forward while the other exposes himself to give covering fire, to the attack manoeuvre of a tank battalion, modern mobile war requires not only team-work but also active solidarity between the troops. The first man takes the greater risk of running forward because he trusts the other will share the risk, and also reduce it by attempting to pin down the enemy with his fire. Every modern army must depend on voluntary cooperation and mutual risk-taking since mobile war cannot be waged by ordering about visible blocks of men in the manner of eighteenth-century foot regiments. And mutual risk-taking can only derive from the deeply felt solidarity of men

---

1 Page 98, "The Wrong War, Why We Lost in Vietnam", by Jeffrey Record, pub US Naval Institute, 1998.

2 p284-286 "The Israeli Army", by Edward Luttwack and Dan Horrowitz, pub Allen Lane, 1975.

3 The kinds of societal problems that lead to poor military performance are not unique to Arab societies. The poor fighting qualities of most of the Italian armed forces in both in the two World Wars are well known. Whilst the Italian big ships and submarines did poorly, the Italian Navy did well in with fast attack craft (MTBs) and with the Special Weapons Department (which had both frogmen and mini-submarines with external crew, which the Royal Navy calls 'chariots'.). "Officers in the [Italian] fleet distanced themselves from the men - and this was common even in submarines where officers enjoyed exceptional privileges and, in some even had their own galley [kitchen] – the Special Weapons Department officers, who included in their number several of high birth, enjoyed close relationships with their men, who often came from humble rural backgrounds. Loyalty was absolute upwards and downwards, and if this stemmed in part from noblesse oblige there was never any sense of inverted snobbery. So long as there was a worthwhile job to do (and this is always the foundation of good morale), class differences worked for, and not against, team spirit amongst the crews [of chariots]." Page 206, "Submarine Warfare Today and Tomorrow", by Capt JE Moore, and Cdr R Compton-Hall, pub Michael Joseph, 1986.

who trust each other with each other's lives. A common hatred for the enemy is not enough. Yehoshafat Harkaby, once head of Israeli Military Intelligence and now a widely respected academic, has explained the Arab weakness in these terms:

> "The crucially important factor in the Arab defeat [of 1967] must be sought in the weakness of the social links which join Arab to Arab. Because of this defect in the social fabric, each Arab soldier, in the critical moments of combat, finds himself fighting not as a member of a team, but as an abandoned individual. Consequently, each individual tends primarily to look after himself, and the unit disintegrates.

"The social defect that induces the anomie observed in Arab soldiers under stress has been described as 'amoral familism' and it is by no means unique to Arab society. Its root cause is perhaps the nature of economic relationships in static societies where, except for windfalls, the overall output does not increase from year to year, since there is no technical progress. Men will cooperate in organised groups if they expect cooperation to yield more than the sum of their individual efforts. But if men feel that more for one can only come from a reduction in the share of another, each will refuse to cooperate since he may well become that other.

"The 'amoral familist' see social relations (other than those within the family) as a zero-sum game; any gains must be somebody else's losses; he will therefore refuse to make sacrifices for others on behalf of the group. Expectation becomes reality since it is self-fulfilling: as brave as any in individual terms, Egyptian soldiers fail to act bravely in groups since each man does not trust the other to share in, and thus reduce, the collective risks faced by the group. Not trusting his fellows to give him covering fire as he advances against the enemy, the single soldier fails to move; seeing his reluctance to accept risks on behalf of the group, the others are confirmed in their mistrust of collective action.

" A brave individual can break the circle within any one small group – and armies are vast collections of many small groups – and thus transform negative individualism into solidarity. The principal duty of junior officers is to do just that: by risking his own life the officer should induce his men to do the same – on behalf of the group. But in Arab society the peasant sees the landlord and office-holder as his natural enemies. Conscripted into the army, the peasant-soldier sees his officers in the guise of landlords and tax-collectors familiar to village life. Just as they expect the tax-collector to be corrupt and make him so by constantly offering him bribes, the peasant soldiers expect their officers to be indifferent to their fate, and makes them so by failing to respond to their leadership.

"These entrenched attitudes do not affect the performance of peasant-soldiers in static warfare where each man can be assigned a fixed firing position and an individual task. The Egyptian soldier has frequently fought steadfastly and well in such conditions. But in mobile warfare, where

mutual confidence is indispensable if one man and one unit are to advance while another man and another unit risk their lives in order to reduce risk for both, the deep mistrust of the amoral familist paralyses the army. Men advance against fire only because of the inner compulsion of their mutual solidarity, unless forced to do so by the whips of their officers as in pre-Napoleonic armies. Where this solidarity does not exist, effective mobile warfare is impossible. Men will run forward against the enemy's fire because their buddies are doing so, and each man feels that he 'cannot let his buddies down'. The amoral familist has no buddies: under stress, he will behave as a solitary individual and no group cohesion underpins the discipline to which he is subjected.

"In practice this means that Arab peasant armies can only be viable military forces in static warfare, where each man can fight on his own and the whole is no more than the sum of the parts. (The most impressive feature of the Egyptian planning in 1973 was the combination of the strategic offensive – the virtual unopposed crossing of the Canal – with the tactical defensive, so that the troops were only required to fight in a static manner to defeat Israeli counter-attacks, which they did – until the second week of the war.)"

3.1.6. How Armed Forces of Nations with Societal Problems can try to Compensate

As mentioned above, some nations have societal problems that tend to produce armed forces, which perform poorly. Poor trust relationships are a feature of this. Historically there have been four main attempted solutions to this:

- Use insurgency warfare (guerrillas/terrorists) to continue the struggle in spite of the inability of conventional armed forces to defeat the enemy. Classic examples of this include the Egyptians against the British in the Canal Zone in the 1950s, the Palestinians against the Israelis, and current operations in Iraq.[1]

- Use brutality to punish and deter people who run away, or who do not participate in attacks. The logic of this is that you make it more dangerous for people who fail to do their duty, than for people who do. Whilst this is probably successful in making people take part in attacks, etc., it is not that obvious that it results in enhanced military capability. As already mentioned, examples of this reportedly include the Soviet Army in parts of World War II, and the German armed forces in 1945.

---

[1] The strategy of insurgency warfare can be pursued whether the number of insurgents is large or small. The actions of any small group can be independent of all other groups (though it does not have to be). Thus the hierarchy of trusting relationships can be smaller and weaker than required for conventional war. Potential suicide bombers are subjected to social pressures, which result in their going through with this 'willingly'.

- Use foreign officers to create an army with better social characteristics than the society the bulk of the army comes from. This was the approach European nations took some of the time with native troops in the 19th and 20th Centuries. The Jordanian Army performed much better than the other Arab armies against Israel in 1948 and 1967. The latter was long after the British officers had left, indicating that the beneficial effect persisted.

- Change society so that the reasons for poor performance no longer apply (or apply less). A good example of this is India, whose society gradually changed from one which modern Indian writers somewhat unfairly call 'feudal' into a bureaucratic democracy. 18th and 19th Century Indian armies were defeated by vastly smaller British armies. However, Indian divisions in World War II, were amongst the British Empire's best troops (e.g. 4 Indian Division). Since the British rule ended in 1947, the Indian armed forces have developed on recognisably British lines, particularly up to battalion level. Once officers reach the rank required for battalion command [colonel], they are subject to societal pressures, which result in divergence from the British model.

3.2 Automation Trust

Automation trust is trust in the satisfactory performance of equipment.

With some equipment it is apparently obvious whether it is working satisfactorily or not (e.g. a tank gun). With other equipment is not so obvious. For example:

- An encryption device may not be secure. This is also a command and control issue.

- A radar warning receiver may be unsatisfactory (i) in that it does not detect the frequencies used by some threat radars, or (ii) it may itself be transmitting a recognisable signature that the enemy may use to target the user.

- Radar intended to warn of the approach of enemy fighters, may be exploited by enemy fighters, who home in on its frequency.

In each of these cases, if the enemy is exploiting a weakness in our equipment, it will be in their interest to conceal this so we continue to use it. In other words, the enemy may reinforce trust by our forces in the unsatisfactory equipment. Stakeholders on our own side may also try to reinforce trust in that equipment.

If the enemy is not exploiting a weakness in a type of equipment, it is possible that he may nevertheless create distrust in that equipment so that its use will be discontinued. Again, this may also be done by our own side in error – perhaps because they need an explanation (or 'scapegoat') for things going wrong.

3.3 Trust and Command and Control

There are a number of issues involving trust and command and control:

- Whether messages are received (Section 3.3.1).
- Security of information, particularly situation reports and orders (Section 3.3.2).
- Veracity of information passed up the command chain (Section 3.3.3).
- Whether subordinates can be trusted to depart from their orders and operate on their own initiative (Section 3.3.4).
- Deception of Command and Control (Section 3.3.5).
- Groupthink (Section 3.3.6).
- The acceptability of Collective Engagement Capability across national boundaries (Section 3.3.7).
- Whether network centricity increases vulnerability to trust attack (Section 3.3.8).

3.3.1. Whether Messages Are Received.

Whether messages are received is important. There are interesting similarities in the verification procedures used with different technologies. These verification procedures allow commanders to have confidence in the system. (i.e. the systems did not purely rely on trust.)

- In the Napoleonic wars armies communicated by messengers on horse-back. To increase the probability of success, several independent messengers would be sent with a message. There was also receipt systems; this could be a simple as the messenger returning with a receipt to prove delivery, or a complex system with receipts at various way-stations allowing someone to track where a message went astray.[1]
- With wireless-telegraphy[2] (WT) the British Army still used the receipt system. i.e. a message was not regarded as sent until one had received

[1] Descriptions of the messenger systems employed in the Peninsular War and the Waterloo Campaign can be found in the following books. "The Man Who Broke Napoleon's Code, the Story of George Scovell", by Mark Urban, pub Faber, 2001. "1815, the Waterloo Campaign, Wellington, his German Allies and the Battles of Ligny and Quatre Bras" by Peter Hofschroer, pub Greenhilll, 1998. "1815, the Waterloo Campaign, the German Victory" by Peter Hofschroer, pub Greenhilll, 1999.

[2] Wireless telegraphy (WT) was radio-frequency communication using codes (e.g. Morse Code) instead of voice. Radio Telegraphy (RT) transmitted spoken words. WT has several advantages: it requires less bandwidth, and it forces people to consider what they want to say before they transmit, which often results in clearer more concise messages.

a receipt of message (which was sent by WT). If the nets were over-crowded, this could result in a message being sent many times before a receipt was received – in extreme cases this could take more than a day.

- With fax systems, fax machines produce a 'receipt of correct transmission' (though this is not the same a receipt from the intended destination). However it is common for people for telephone (or more recently email) to warn people of the fax, and to enquire whether it has arrived.

- Modern email systems have receipt systems (though mistakes in their implementation make them unreliable[1]). Again it is common for people to ask either for a reply acknowledging receipt or to telephone enquiring whether it has arrived. If a recipient has several email addresses, it is not uncommon for people to sent the same messages to each address to increase the probability of it being read.

These measures of requiring a receipt and of sending multiple messages are employed because people have low trust in message delivery. They add to the number of messages being transmitted on the system. Perversely, the more overloaded the system, the greater the need for receipts and multiple transmission of messages.

Clearly this is an area where trust attack is possible – degrading the functioning of communications (by jamming radios, or cutting communication cables) will reduce confidence in the communication system, and thus cause people to behave in a way that increases message traffic (due to transmission of receipts and multiple copies of messages).

3.3.2. Security of Information.

Whether one is communicating by messenger, radio or through wires, there is a danger that the enemy will receive messages intended for our troops. An attempted solution to this is encryption.

Historically encryption has increased the time it takes to compose and transmit and receive a message. It is also necessary to equip people to do this.

However codes can be broken – including apparently unbreakable codes. This can give the enemy a significant information advantage – which can be maintained by trust attack – in this case by trying to reinforce trust in the code. A common method is to not use information unless there is an independent source - in World War II, some aerial reconnaissance missions were undertaken solely to provide a plausible alternative source of the

[1] On Outlook-based systems the author has experience of receiving 'message deleted unread' receipts, with respect of messages where the recipient has sent a reply.

information, thus preserving the secret that the British were reading German codes.[1]

3.3.3. Veracity of Information.

"If the channel of communication in the armed forces becomes a channel for communicating exaggerated reports and lies… none of the levels [of command]… can act from knowledge of the situation. Decisions are therefore faulty. Subordinate levels are caught in a vicious circle: on the one hand they know that command prefers to receive favorable reports – even if this is false boasting – responsively, they supply them. On the other hand, they cannot trust the orders of their command since they know they are based on incorrect data."[2]

Even in the British Army there have been problems with over-hopeful messages being sent back. An examination of war diaries for World War II shows that it is not uncommon for success signals in battalion attacks to be sent too early (i.e. before the objective has been fully taken).

Israeli sources claim (with considerable justification) that Arab armed forces suffer particularly from the problem of reports being unduly optimistic.

3.3.4. Whether Subordinates can be Trusted to Depart from Their Orders and Operate on their own Initiative.

In the 1973 Arab-Israeli war, Israeli forces crossed the Suez Canal at 0100 hrs on 16th October 1973. During the 16th, the Egyptians did not seriously counter-attack the forces that had crossed the canal, though they made determined counter-attacks on the approach route to the canal. The Egyptian failure to destroy the Israeli bridgehead over the canal whilst they had a chance, caused Egypt to lose the war.

The Egyptian behaviour was due to way the Egyptian command system worked, and the clever exploitation of this by General Ariel Sharon (who commanded the Israeli division that crossed the canal on the 16th). Egyptian divisions followed their prepared plans with dogged persistence

---

[1] British code-breaking successes in both the Peninsular War and World War II were kept secret long after these wars were over. The reason was to that the enemy encryption methods broken were regarded as likely to be used by foreign powers in the future. It was therefore an advantage to maintain foreign trust in these methods, so that we take advantage of our ability to decipher them in the future.

[2] "Basic factors of the Arab Collapse During the Six Day War", by Yehoshafat Harkaby, pages 678-9 "Orbis", Fall 1967. Quoted in p286-287 "The Israeli Army", by Edward Luttwack and Dan Horrowitz, pub Allen Lane, 1975.

and great rigidity of purpose. They were not trusted to show initiative by doing something that had neither been ordered nor planned.[1]

There are two rival concepts of command:

- *Befehlstaktik*. Also known as 'Restrictive Command'. The soldier "must comply with an order given him by others, with no chance for him to fall back on his own initiative and skill, either in adapting himself, or in exploiting situations as they come up."[2] Befehstaktik is the traditional method of command used by the British and US Armies,[3] and is still used by many armies. This was the method used by the Egyptian Army in 1973.

- *Auftragstaktik*. Also known as 'Directive' or 'Mission Command'.[4] "A mission is ordered and the officer is left with the freedom to carry out the mission assigned to him, and so he feels responsible for the actions which are suggested to him by his intelligence, his enterprise and his capabilities."[5] Auftragstaktik was first introduced in the Prussian Army in 1813 and had been used by the Prussian/German Army ever since. It was originally adopted in an era of poor communications, because it was realised that circumstances change, and that a unit's orders may no longer be applicable, and that opportunities would be missed if a unit had to report the situation to higher command, and await orders before responding. The British Army gradually adopted Auftragstaktik in the 1980s. There was an earlier unsuccessful British attempt to adopt it in the late 19th Century.[6]

Auftragstaktik requires greater trust in subordinates. They also need to be trained to understand what is expected of them.

---

1 Page 382 "The Israeli Army", by Edward Luttwack and Dan Horrowitz.

2 "German Tactics in the Italian Campaign", by Gerhard Muhm, pub Circolo Fratelli Rosselli. http://www.larchivio.org/xoom/gerhardmuhm2.htm

3 Currently the US Army and Air Force use extremely detailed orders, which seem quite alien to officers from armies that use Auftragstaktik. Whilst the US Army says that it espouses Auftragstaktik, its enacted behaviour suggests Befehlstaktik.

4 See also Chapter 6, "The Big Issue: Command and Combat in the Information Age", edited by David Potts, pub Strategic and Combat Studies Institute, March 2002. http://www.dodccrp.org/publications/pdf/Potts_Big_Issue.pdf

5 "German Tactics in the Italian Campaign", by Gerhard Muhm.

6 There are a number of 'lessons learned' papers in British divisional war diaries for 1918, which lament the long and very detailed orders used by the British Army at the time (which used Befehlstaktik). However, the papers go on to say that given the way that the British Army had been expanded during World War I, and the training of the troops, there seemed no other alternative.

3.3.5. Deception of C2

There are a number of forms of command and control deception:

- *Infiltration of false people into the organisation*. An obvious example are spies and saboteurs. Another example was the famous Panzerbrigade 150 (Skorzeny) in the Battle of the Bulge in December 1944.[1] In counter-insurgency warfare, it is normal to use small groups of pseudo-terrorists who pass themselves off as terrorists; some newly captured terrorists are coerced into joining the pseudo-terrorists, which makes it difficult to identify who is whom.[2] [3]

- *Planting of false orders*. In the latter part of World War II RAF Bomber Command used aircraft known as 'ABC', which accompanied bomber formations and tried to broadcast false orders to German night-fighters to confuse them. The British Army also used this technique to cause distrust.

---

[1] Panzerbrigade 150 (Skorzeny) was a German formation intended to cause chaos to assist the German offensive. They wore US uniforms, either captured US vehicles and vehicles modified to make them look American. Many spoke English. "The best English-speaking volunteers were selected to a special commando unit, know as Einheit Stielau... This unit was be sent in in small units, and destroy fuel dumps, bridges ammunition, do reconnaissance missions seep inside the Allied territory, and give out fake orders and spread confusion." Captured members of Panzerbrigade 150 said that their mission was to capture General Dwight D Eisenhower and his staff. "Panzerbrigade 150 - Skorzenys secret formation in the Ardennes", http://www.panzerworld.net/pzdivs/pzb150.html

[2] An easily read and accessible account of pseudo-terrorist operations is a book by the former commanding officer of the Selous Scouts (the Rhodesian Army's pseudo-terrorist unit). "Selous Scouts, Top Secret War", by Lt Col RR Daly as told to P Stiff, pub hardback 1982, and Galago paperback 1983.

[3] "Gen George Crook developed the tactic of inserting small teams from friendly Apache tribes into the sanctuaries of insurgent Apaches to neutralize them, to psychologically unhinge them, and to sap their will. This technique subsequently emerged in one form or another in the Philippines, during the Banana Wars, and during the Vietnam War." [The 'Banana Wars' were various conflicts in the Caribbean where the US intervened between 1989 and 1934.]

The US armed forces pseudo-terrorists in the Vietnam War were organised under "the Phuong Hoang program, or Phoenix. The purpose of Phoenix was to neutralise the Viet Cong infrastructure, and although the program received some negative attention in the instances when it was abused, its use of former Viet Cong and indigenous Provisional Reconnaissance Units to root out the enemy's shadow government was very effective."

"Back to the Street without Joy: Counterinsurgency Lessons from Vietnam and Other Small Wars", by Robert M Cassidy, Parameters, US Army War College Quarterly, Volume XXXIV No 2, Summer 2004.

According to the above article an account of various US Army pseudo-operations is contained in pages 55-92, "US Army Counterinsurgency and Contingency Operations Doctrine 1860-1941", by Andrew J Birttle, pub Washington US Army Center of Military History, 1988.

- *Planting of false information.* This is a standard form of deception, it may be done with false radio traffic, decoys (including radar decoys), or passing information through the enemy spy network including deception messages on telephone. Military offensives often have a deception plan. A key feature of any such deception is to ensure that as few people as possible know about the deception. For instance, with Operation DESERT STORM, many people knew the deception plan – but thought that it was the real plan.

- *Concealment of information.* If the enemy is to be given false information through his spies and sensors, then true information needs to be concealed. One of the most important pieces of information to conceal is that one has broken his codes.[1]

Even when these fail, they can cause distrust. The more convincing they are, the greater the damage to trust. Indeed the knowledge that the enemy might be trying to do these things will cause distrust.[2]

Whilst they are normally done by the enemy – they sometimes done by allies. The planting of false information and concealment of information may even be done one's own people, sometimes for reasons discussed in Section 3.3.6. False orders can arise through panic (often because people lie and pretend that they have orders that they have not got, or make false claims about why they are running away).

3.3.6. Groupthink

Groupthink is a concept originated by Irving Janis (a Yale social psychologist).[1] He "originally defined groupthink as 'a mode of thinking

---

[1] For instance, during World War II the British successfully concealed that they had broken the German Enigma code. The British policy was not to make the maximum use of the information gained through Enigma, and to ensure that there was always an alternative explanation available for how the British knew (i.e. maintaining German trust in Enigma). For instance, with German resupply ships in the Atlantic in June 1941, the British decided to attack only 6 out of 8 (unfortunately the 2 that were to be spared were found by chance by British forces and eliminated). With enemy resupply convoys in the Mediterranean, the British sent reconnaissance flights in their expected direction, which could then be blamed for the convoy's detection.

Page 347 "Germany and the Second World War, Volume VI", by Horst Boog, et al, pub in English by Clarendon Press, 2001.

[2] In the Falklands Campaign the BBC broadcast news of 2 Para's attack on Goose Green before it happened. Argentine forces received this information but did not act on it, because they did not trust it.

During the German offensive in the West in 1940, there was a widespread belief in France that the Germans were aided by spies, saboteurs and traitors. See, for instance, pages 520-2, "To Lose a Battle, France 1940", by Alistair Horne, pub Macmillan 1969, and Penguin 1987.

that people engage in when they are deeply involved in a cohesive in-group, when the members' strivings for unanimity override their motivation to realistically appraise alternative courses of action.' According to his definition, groupthink occurs only when cohesiveness is high. It requires that members share a strong 'we-feeling' of solidarity and desire to maintain relationships within the group at all costs. When colleagues operate in a groupthink mode, they automatically apply the 'preserve group harmony' test to every decision they face."

"Most students of group process regard members' mutual attraction to each other as an asset. Marvin Shaw, a University of Florida psychologist and the author of a leading text in the field, states this conviction in the form of a general hypothesis that has received widespread research support: 'High-cohesive groups are more effective than low-cohesive groups in achieving their respective goals.' But Janis consistently held that the 'superglue' of solidarity that bonds people together often causes their mental process to get stuck:

> "The more amiability and esprit de corps among members of a policy-making in-group, the greater is the danger that independent critical thinking will be replaced by groupthink. . . . The social constraint consists of the members' strong wish to preserve the harmony of the group, which inclines them to avoid creating any discordant arguments or schisms.'

"Janis was convinced that the concurrence-seeking tendency of close-knit groups can cause them to make inferior decisions."[2]

One of the features of groupthink is an unwillingness to consider alternatives to the desired decision. Information that goes against the desired decision tends to be ignored. People who make difficulties, for instance raising objections, tend to be got rid of because they do not fit in. (In other words, people tend to have great trust in the desired decision, and to distrust contradictory information/people.)[3]

---

[1] "Victims of groupthink", by Irving Janis, pub Houghton Mifflin, 1982. The second edition was entitled: "Groupthink: Psychological studies of policy decisions and fiascos".

[2] Chapter 18, "A First Look at Communication Theory" by Em Griffin, pub McGraw-Hill, 1997. http://www.afirstlook.com/archive/groupthink.cfm?source=archther

[3] A good military example of groupthink was the behaviour of the staff of the 1 British Airborne Corps in September 1944. The desired decision was a landing by three airborne divisions at seven locations. One of those locations was Arnhem. Two important facts were suppressed during the planning, which caused major problems during the operation for the division that landed at Arnhem:

- The divisional signals staff were worried that their 'No 22' radios might not have sufficient range. The did not raise these concerns because they did not want to 'rock the boat', and in any case they believed there would be mitigating factors: the problem would only be for a few hours (it wasn't), and that another unit had longer range radios (they got damaged).

3.3.7. The Acceptability of Collective Engagement Capability across National Boundaries

Collective Engagement Capability (CEC) is a new network-centric ability, which has been created for fleet air defence in the US Navy. It will be introduced into other navies, and in time to other warfare areas.

An enemy aircraft or missile is detected and tracked by radar, and missiles are fired at the aircraft or missile. With CEC, the platform that makes the firing-decision does not have to be the one with the radar, or the one with the missiles. They can be three separate platforms with data-links.

With traditional methods of fire-control, the vessel firing missile would track the target with its own radar, and make the decision whether to fire itself. Even if ordered to fire by the task group commander, the ship would still have to decide whether to comply.

In a multi-national task group, different coalition partners' ships could have different Rules of Engagement (RoE).

- With traditional methods of fire-control, the firing ship would clearly be subject to national RoE. These could override an order from the task group commander to open fire.

- With CEC, the situation is less clear. All the ships in the task group may contribute to the radar track of the target. The platform that makes the decision to fire may be of a different nationality than the one carrying the missiles. Missiles may be fired from a ship without any decision by that ship.

With CEC, there are issues of trust and different national RoEs. There are also issues of on-line trust between platforms.

3.3.8. Does Network-Centricity Increase Vulnerability to Trust Attack

Network-centricity ought to lead to more efficient use of combat assets. However it creates five areas of vulnerability, where trust attack is important:

- Overall intelligence reports were optimistic. There was some vague evidence from Dutch sources that there were two German panzer divisions near Arnhem. The intelligence major in the Corps HQ raised doubts about the operation, and tried to confirm the Dutch intelligence with photo-reconnaissance (which was inconclusive – tanks appeared on only 5 of the hundreds of photos taken). Members of the HQ staff decided that the major must be suffering from nervous exhaustion brought on by over-work; the corps medical officer sent him on leave on those grounds.

Pages 161-2 (radios) and 114-7 and 141-3 (intelligence), "A Bridge Too Far", by Cornelius Ryan, pub Hamilton 1974, paperback Coronet, 1975.

- The technological process required for network-centricity may be exploited by the enemy. The enemy may be expected to reinforce trust in the process, so that they can continue to exploit this.[1]

- Centralised direction of assets makes it worth the enemy doing deception operations so that our assets are doing the wrong thing.[2]

- Network-centric command involves far more communication than traditional methods. These communications make be disrupted or targeted.

  – Traditional methods of disruption include radio jamming, cutting communication cables with artillery, or attacking radio stations with aircraft or artillery.[3] In a system that uses internet protocols, it might be possible to do the kinds of attacks that are seen on the internet.[4] Disruption attacks trust in the working of the system.

  – Targeting of radio communications may be done using aircraft, missiles, or artillery. In addition to the benefits of destroying assets and killing people, this deters people from communicating (i.e. it attacks trust in the ability to use the system safely).

- Network-centric command can involve huge amounts of information flowing around the system. It will be difficult to process this information; people will have to be selective. Depending on how the organisation and its information systems are structured, the greater volume of information could make it easier to lapse into groupthink

---

[1] During the Battle of the Atlantic in World War II, a form of network-centric command directed the operations of German U-boats. The British used radio direction-finding to locate U-boats when they transmitted radio messages to HQ. (The Germans knew about this weakness.) Part way through the war, the British started to break the German Enigma code used for messages. (As already mentioned, this was successfully concealed from the Germans.)

[2] During the latter part of 1943, the German night-fighter force started to be operated under a network-centric system known as 'Zahme Sau'. Information would be collected both from radar, sigint, and German aircraft, and used to direct night-fighters on to the bomber stream. The RAF used a number of deception methods to attack this method:

- They instituted decoy raids by small numbers of aircraft, dropping chaff to simulate greater numbers of aircraft than there really were.
- They tried having two bomber streams instead of one, to confuse the Germans.
- Electronic countermeasure aircraft called 'ABC' accompanied the bombers. Some of the time these jammed German signals. Some of the time they issued false orders.

[3] If people move over to laser communications, presumably armed forces will start using smoke designed to absorb or disrupt the frequencies used.

[4] It will be impossible to guarantee that the enemy will not get access to the system - either through spies, reverse engineering, or capture of equipment. All of these things have been done before.

(see Section 3.3.6). Whilst this represents a form of unintended internal attack on trust, many successful deception operations involve telling the enemy what he wants to believe anyway. Therefore vulnerability here makes us more vulnerable to trust attack both from the enemy, and defects in our own organisation.

- Network-centric command also makes it easier for very senior decision-makers to interfere in low-level decisions. This is sometimes known as the long screwdriver. This tendency to micro-manage is a problem. The high-level commander is not doing his own job properly. He cripples his subordinates by depriving them of initiative (because he is showing that he does not trust them). He is often not as well placed to make the right low-level decision as the man on the ground.

3.4 Political Trust

High Level. It is possible to lose in war through loss of political trust, in spite of military success. A good example of this was the 1956 Suez Crisis. British and French forces undertook military operations against Egypt, giving untruthful reasons for the action. There was widespread disbelief in Anglo-French claims. The lack of confidence (distrust) in the government, led to the Anglo-French forces withdrawing in humiliation, with the British Prime Minister retiring afterwards. This is an example of people using the truth to destroy trust.

There is also widespread distrust in the truthfulness of Allied statements of why they invaded Iraq in 2003. The Spanish government lost the March 2004 general election in part because of Iraq, and in part because of distrusted claims that Basque separatists (ETA) were responsible for bombs attacks in Madrid.

The Vietnam War was also lost on a political level in the USA. People no longer trusted that it was worthwhile. A turning point was the 1968 Tet Offensive. In military terms this was a disaster for the communists. However, it seemed to prove that US Government claims about their degree of success in the war should not be trusted. As a result President Lyndon Johnson decided not to go for re-election, and to pursue a strategy of negotiating a US withdrawal from Vietnam. This policy was continued by Johnson's successor, Richard Nixon.

It is also possible that powerful armed forces may fail to deter, if potential opponents do not believe they will be used. British forces were unable to deter the Falklands War, because the Argentine Government did not believe that Britain would go to war over the Falklands. One of the reasons for the failure to reach a negotiated settlement was that it was difficult to believe that the Falklands Task Force was anything but a bluff.[1]

[1] The author was at university at the time. Having grown up in the 1970s, it seemed that modern British Governments might threaten force, but ultimately they always seemed to back down.

Low Level. Low level political trust differs from high level political trust in that with low level political trust the key actors are individual ordinary men and women, whereas with high level political trust the key actors are governments, multinational corporations, major charities, etc.

Low level political trust is especially important in counter-insurgency campaigns.

Ordinary people are concerned about their families and their future. In a counter-insurgency (such as the current campaign in Iraq) the occupying power (US) is currently very powerful, whereas local resistance (Baath, etc.) are weak.

- If ordinary people trust that the occupying power is permanent, then it may be worth co-operating with them to build a better society. Since the occupying power is rich, this can be rewarding.

- But if ordinary people believe that the occupying power is only there temporarily, then in a few years time they will be gone. That will probably leave the local resistance in a position of strength to seek revenge on those who co-operated with the occupying power. It therefore becomes dangerous to co-operate with the occupying power.

- If the occupying power wishes to leave a friendly government in place after they leave, they need to inspire trust in the permanence of that government. This is partly done by choosing the right people to form the government, and partly through guarantees of support. Historically, it is common for the friendly successor government to have policies that are a compromise with the sentiments of the politically active part of the local population.[1] This still causes problems of trust for people who want to co-operate with the occupying power now, because even if the occupying power succeeds in setting up a friendly successor government, this successor may still be less-than-friendly to those who collaborated with the occupying power.

Mrs Thatcher's government seemed no different. In the 1979 Conservative Manifesto there was a promise to recognise Rhodesia if certain conditions were met. The conditions were met, but recognition was not forthcoming (it would have been unpopular with the Commonwealth).

[1] A good example of this is the West German state set up to take over the government of western Germany from the Western Allies. The West German government reduced the severity of the de-nazification programmes, and some former members of the Gestapo were able to take legal action to restore their pensions, including increments gained for their part in the Holocaust. By the 1950s Germans who had served on Allied de-nazification courts were "socially ostracized or economically penalized in their own communities."

"Occupation Hazards, Myths of 1945 and US Iraq Policy", by Douglas Porch, "The National Interest", Summer 2003. "The Nazi Terror, Gestapo, Jews and Ordinary Germans", by Eric Johnson, pub J Murray, 1999.

It seems to have been a standard tactic for communist insurgents to target native people who co-operated with the government. One technique used in Vietnam was to kill the entire families of 'collaborators'. In villages in Rhodesia, the communist terrorists would force residents of the village to hack 'collaborators' to death with agricultural implements such as hoes. This meant that the people of the village shared the guilt of the killings, and was both shocking and intimidating.

It is therefore not very surprising that people, who do wish to co-operate with the occupying power, often seek to hedge their bets by also co-operating with the resistance. This makes them hard to trust.

4 MoE on Trust Attack in Context of C2

The appropriate Measures of Effectiveness (MoE) for trust attack depend on what we are trying to achieve.[1] In Effects Based Operations it is not appropriate to have MoEs solely based on numbers of enemy tanks destroyed, etc (i.e. 'bean counting'). The MoEs in this section are effects based; i.e. they attribute scores to different effects on the enemy.[2]

A definition of trust attack is given in Section 1.2.4. In general terms someone trying to attack trust is trying to do one or more of the following:

- Reinforcing trust, usually "I trust false information".
- Destroying and degrading trust, usually "I don't trust true information" and "I need more time to decide", but occasionally "I don't trust the false information people want me to believe".
- Making the system unworkable, "I don't trust the system and won't use it".

There is nothing incongruous about attempting to reinforce trust in one part of the system, whilst at the same time as degrading trust in other parts. This is a basic form of deception.

MoE have been worked out for the following potential areas of trust attack (which have been classified in terms of the above):

- Make System Appear not to Work (i.e. make unworkable)

---

[1] "Measure of Effectiveness (MoE): An objective metric used to assess the level of success achieved for a given desired effect." Page 12, "MoE & EBO in HQ ARRC", by Hugh Richardson, Head OAB HQ ARRC, ISMOR paper, September 2004.

[2] The argument as to whether you should measure effectiveness in terms of effects achieved or level of destruction achieved is not new. See paragraphs 21-22, "Operation MUSKETEER", DD.Ops(Tac)/TS.301/III, 19th February 1957, PRO Reference AIR8/2111.

During the Vietnam War the US Department of Defense focussed on quantifiable measures of military power, and countable measures of progress such as sorties flown, bomb tonnages dropped, artillery shells fired, and enemy killed. US Secretary of Defense, Robert "MacNamara believed that most things could be precisely measured, and that those that could not probably didn't matter much anyway." This approach was unsuccessful. Pages 50-52, "The Wrong War, Why We Lost in Vietnam", by Jeffrey Record, pub US Naval Institute, 1998.

- Attack Battle Damage Assessment (i.e. reinforce and degrade different areas)
- Make System Appear Dangerous (i.e. degrade)
- Maintain Confidence in System (i.e. reinforce)
- Attack Appreciation of Situation (i.e. reinforce and/or degrade)
- Attack IFF (i.e. degrade/make unworkable)
- Degrade Trust in the System (i.e. degrade)

4.1 Structure of MoEs

Colour Coding of Results. The various end results in the MoEs have been colour coded. Red is bad, and green is good, with yellow intermediate. In some cases the colour code has a different colour border and diagonal line – this to represent cases where the end result could be one thing or another. These cases will be explained in each section.

Quantification of Results. It would be possible to ascribe arbitrary scores to each end result. The author has not done this to avoid giving false precision to the results, or expressing a preference between two end results, where in reality one's preference could only be assessed with a more precise and less generalised description of the result.

Who is the Enemy/Target. It is assumed in the MoEs that the targets of trust attack are enemy forces.

If trust in our own forces is being attacked by mistaken or undesirable behaviours or policies in our own forces, then the end results in the MoEs should be reversed. (It is bad that we are doing this to ourselves.)

It is also possible that third parties are attacking trust. Whilst the MoEs give a measure of effectiveness for our point of view; this MoE probably does not relate to the preferences of a neutral third party.

Target Behaviour Columns. The columns listed under 'Target behaviour' list different things the enemy/target may do. They have been done like this because behaviours are not necessarily mutually exclusive.

Consequence Column. This column is a summary of the effect. It should be read in conjunction with the 'target behaviour' columns.

Numbered Rows. Different outcomes have been numbered. The numbers are for reference; they do not indicate a preference.

Are These Really Measures of Effectiveness? These measures of effectiveness do not look like MoEs based on percentage of tanks destroyed and numbers of enemy killed. But they really are MoEs:

- They are measures. The colour coding is a score. If a user wants to numericise these, he can.

- The effects are shown in the 'consequence' and 'target behaviour' columns.

With an MoE, what one wants is a graduated indicator (or set of indicators), in which progress in one direction always represents improvement ('monotonic' behaviour).[1]

- For attrition warfare it is relatively easy to define simple concepts of effectiveness such as enemy casualties or runways cratered. Though it is worth adding that accurate measurement of these has been a problem in the past – the tendency has been to grossly over-estimate the damage and casualties inflicted on the enemy. Traditional OA models have produced these data as outputs (generally because the design concepts had attrition warfare in mind).

- For Effects Based Operations, such simple concepts of effectiveness are not readily applicable. The effects that military operations are trying to achieve in the modern world are normally behavioural. This is particularly true of the use of air-power. Indeed, attrition-based measures tend to underestimate the effectiveness of air-power. The measures, which the author believes are most suitable for Effects Based Operations, are defined as a set of Boolean-valued target behaviour variables. These are a lot easier to assess in military operations, than attrition based measures. It is conceded that some OA models could have difficulty supporting such measures; though if this is the case the suitability of such models for assessment of Effects Based Operations is doubtful.

[1] An example of a monotonic indicator is income; having a greater income is normally regarded as better.

An example of an indicator, which is *not* monotonic is body temperature. If one's body temperature is within a certain range that is good. If body temperature is higher *or* lower than that range that is bad.

4.2 Make System Appear not to Work

Figure 4.1 shows MoEs for trust attack where the intended effect is to make it appear that the enemy system does not work. Examples of systems that might be attacked in this way include encryption systems, air defence command systems.[1]

There are two ambiguous cases (7 and 8), where the results could be good or bad. With an encryption system these could occur if the enemy allows us to think we have succeeded, and then uses this knowledge as part of a deception plan for one of his operations.

		Target Behaviour						
	Colour Coding	Enemy continues using system.	Enemy temporarily suspends using system.	Enemy abandons system.	Enemy investigates system.	Enemy modifies system.	Enemy uses system to feed false information to us.	**Consequence**
1		TRUE						Bad. Attack failed.
2		TRUE			TRUE			Quite bad. But at least enemy wasted effort on investigation.
3			TRUE		TRUE			Temporary benefit.
4			TRUE		TRUE	TRUE		Temporary benefit.
5				TRUE	TRUE			Good.
6				TRUE	TRUE	TRUE		Good.
7				TRUE	TRUE		TRUE	Appears good, but may lead to bad consequences if enemy deceives
8				TRUE	TRUE	TRUE	TRUE	Appears good, but may lead to bad consequences if enemy deceives

Figure 4.1 MoEs for Trust Attack to Make the Enemy System Appear Not to Work.[2]

[1] A historical example damaging trust in the ability of an air defence command system to work is that of RAF Bomber Command's use of 'Window' (chaff) starting in July 1943 against the Himmelbett system used by the Germans to control their night-fighters. Trust was damaged by filling the radar screens with obscurants. Whilst this did damage trust, it also made the system work poorly.

[2] The combination of 'enemy modifies system' and 'enemy abandons system' in Rows 6 and 8 is possible. It can happen because people lose trust in the system despite the modification (e.g. German

4.3 Attack Battle Damage Assessment

	Target Behaviour						
	Colour Coding	Own asset continues being bombed	Bombing intensity increases	Bombing intensity decreases	Similar friendly assets continue being bombed	Enemy stops bombing this type of asset	**Consequence**
1		TRUE	TRUE		TRUE		Major failure
2		TRUE			TRUE		Failure
3		TRUE		TRUE	TRUE		Limited partial success
4					TRUE		Partial success
5						TRUE	Success

Figure 4.2 MoEs for Trust Attack on Battle Damage Assessment to Cause Enemy to Stop Attacking Certain Targets.

night-fighters could home in on the Lancaster's tail-warning radar; a modification did not fix the problem). It can also happen for budgetary reasons or because of policy changes.

	Target Behaviour						
	Colour Coding	Own asset continues being bombed	Bombing intensity increases	Bombing intensity decreases	Similar friendly assets continue being bombed	Enemy stops bombing this type of asset	Consequence
1		TRUE	TRUE		TRUE		Major success
2		TRUE			TRUE		Success
3		TRUE		TRUE	TRUE		Partial success
4					TRUE		Limited partial success
5						TRUE	Failure

Figure 4.3 MoEs for Trust Attack on Battle Damage Assessment to Cause Enemy to Continue or Intensity Efforts on Current Targets

Figures 4.2 and 4.3 show MoEs for attack of trust for battle damage assessment. The reason there are two MoEs, is that the objective might either be for the enemy to stop attacking certain target (Figure 4.2), or to continue or intensify attacks on these targets. These diagrams are identical apart from the preferences. In the past, Air Forces have often intensified their efforts when they have found that the damage they were inflicting was not defeating the enemy. This would suggest that concealing bomb damage might lead to increased bombing. If targets appear to be knocked out, they are less likely to be attacked in the future.

Battle damage assessment is an important part of effects based operations for air campaigns. By attacking battle damage assessment one can try to influence the enemy air campaign.

- During an air campaign it is common for the defenders to conceal their losses so that the enemy does not know what is working, and because it makes it difficult for the enemy to exploit his successes if he does not know about them. In the 1982 Falklands Campaign it would have been desirable to have concealed that many Argentine bombs were not detonating in our ships.[1]

[1] Page 216 "The Royal Navy and the Falklands War", by David Brown, pub Leo Cooper, 1987.

- The Argentine defenders of Port Stanley in 1982 dug false craters at the airfield to make it seem as if our bombing attacks had been more successful than they were (and thus make further bombing redundant).

4.4 Make System Appear Dangerous

		Target Behaviour						
	Colour Coding	Enemy continues using system as before	Enemy only uses system in safe areas	Enemy stops using system	Enemy adopts modified or replacement system	Enemy temporarily abandons this capability	Enemy abandons this capability	**Consequence**
1		TRUE						Failure
2		TRUE				TRUE		Enemy has temporary capability gap, during investigation
3				TRUE	TRUE			Enemy forced to use resources on new/modified equipment.
4				TRUE	TRUE	TRUE		Enemy has temporary capability gap, during investigation or period before modified or new equipment's in service date Enemy forced to use resources on new/modified
5			TRUE					Geographically limited success
6				TRUE			TRUE	Total success

Figure 4.4 MoEs for Trust Attack to Make the Enemy System Appear Dangerous.

Figure 4.4 shows MoEs for trust attack to make enemy believe that his systems are dangerous to use. Many examples of this involve radio-frequency transmissions, either in radios or radar. A good example would be British success in deterring German units from using radio for unit communication in the front-line area in Normandy in June-August 1944.[1]

[1] Translations of captured German documents in intelligence summaries in War Dairy HQ GS 7 Armoured Division, August 1944. PRO referenceWO171/440. (Notes from these documents are in file "Notes on 326 Div doc.doc".)

4.5 Maintain Confidence in System

		Target Behaviour						
	Colour Coding	Enemy continues using system as before	Enemy only uses system in safe areas	Enemy stops using system	Enemy adopts modified or replacement system	Enemy temporarily abandons this capability	Enemy abandons this capability	Consequence
1		TRUE						Success. We continue to exploit enemy system
2		TRUE				TRUE		Temporary gap in our ability to exploit enemy system
3				TRUE	TRUE			Failure. However, we may learn to expoit the new or modified system, so the problem may only be temporary
4				TRUE	TRUE	TRUE		Failure. However, we may learn to expoit the new or modified system, so the problem may only be temporary
5			TRUE					Failure, unless we are able to exploit the system in areas the enemy believes to be safe
6				TRUE			TRUE	Failure

Figure 4.5 MoEs for Trust Attack to Maintain Enemy Confidence in his System.

Figure 4.5 shows MoEs for trust attack to make enemy believe that he should have confidence in his systems. Examples of this would include an encryption system that we had broken, a navigation system that we were able to corrupt, or information systems that had been compromised by spy-ware and file-sharing programmes.

Note that there are three ambiguous cases. (3) and (4) represent failure in the short term; however if we are learn to exploit the new system, the result may not be so bad. (5) represents a system that the enemy learns can no longer be used safely within range of us; if our capabilities are greater than he knows, it may still be possible to exploit the system in what he deems safe areas.

4.6 Attack Appreciation of Situation

Figures 4.6 and 4.7 show MoEs for attacking trust with respect of the enemy appreciation of the situation. In land warfare people often wish to

make the enemy overestimate the threat from us where our forces are weak, and underestimate it, where our forces are strong. That encourages the enemy to make a sub-optimal distribution of forces, and makes it easier to conceal our intentions, and thus get surprise.

		Target Behaviour						
	Colour Coding	Enemy strength in sector underestimated	Enemy strength in sector correctly appreciated	Enemy strength in sector exaggerated	Own/Allied strength in sector underestimated	Own/Allied strength in sector correctly appreciated	Own/Allied strength in sector exaggerated	**Consequence**
1		TRUE					TRUE	Enemy believes he is in a better situation than he is in
2		TRUE				TRUE		Enemy believes he is in a better situation than he is in
3			TRUE				TRUE	Enemy believes he is in a better situation than he is in
4			TRUE			TRUE		Enemy appreciation correct
5			TRUE		TRUE			Enemy believes he is in a worse situation than he is in
6				TRUE		TRUE		Enemy believes he is in a worse situation than he is in
7				TRUE	TRUE			Enemy believes he is in a worse situation than he is in

Figure 4.6 MoEs for Trust Attack to Make the Enemy Believe his Situation is More Favourable Than It Is.

Figures 4.6 and 4.7 show a number of consequences in terms of the effect on the appreciation. However the appreciation of the situation will lead to command decisions. Potential faulty command decisions may include:

- Requiring huge reinforcements before launching an offensive (due to an over-estimate of enemy abilities – e.g. Operation DESERT SHIELD/STORM).

- Launching offensives in circumstances where defeat is inevitable (due to an overly optimistic appreciation).

- Assigning troops tasks beyond their capabilities (due to an overly favourable appreciation).

- Under-utilising troops whose capabilities are under-appreciated.[1]

		Target Behaviour						
	Colour Coding	Enemy strength in sector underestimated	Enemy strength in sector correctly appreciated	Enemy strength in sector exaggerated	Own/Allied strength in sector underestimated	Own/Allied strength in sector correctly appreciated	Own/Allied strength in sector exaggerated	**Consequence**
1		TRUE					TRUE	Enemy believes he is in a better situation than he is in
2		TRUE				TRUE		Enemy believes he is in a better situation than he is in
3			TRUE				TRUE	Enemy believes he is in a better situation than he is in
4			TRUE			TRUE		Enemy appreciation correct
5			TRUE		TRUE			Enemy believes he is in a worse situation than he is in
6				TRUE		TRUE		Enemy believes he is in a worse situation than he is in
7				TRUE	TRUE			Enemy believes he is in a worse situation than he is in

Figure 4.7 MoEs for Trust Attack to Make the Enemy Believe his Situation is Worse Than It Is.

[1] Allied plans for the invasion of Sicily in 1943 were for the US Army to act as flank-guard for a British offensive. This was because the British had formed a low opinion of US troops in the North African Campaign – a contemporary British phrase for US troops was 'our Italians'. One of the reasons General Patton launched the US offensive that took him to Palermo and Messina was to demonstrate the true capabilities of US troops, thus restoring trust in them.

4.7 Attack IFF

		Target Behaviour						
	Colour Coding	Enemy IFF used all the time	Enemy IFF used in safe areas only	Enemy uses restrictive RoE	Enemy has increased levels of friendly fire	Slight disruption to enemy organisation	Serious disruption to enemy organisation	Consequence
1		TRUE						Failure
2			TRUE					Attack of trust partially successful, but no good consequences
3				TRUE				Attack of trust partially successful, but few or no good consequences
4			TRUE		TRUE			Attack of trust partially successful, and some benefits
5				TRUE	TRUE			Attack of trust partially successful, and some benefits
6				TRUE	TRUE	TRUE		Limited success
7					TRUE	TRUE		Limited success
8				TRUE	TRUE		TRUE	Major success
9					TRUE		TRUE	Major success

Figure 4.8 MoEs for Trust Attack of IFF.

Another target for trust attack is the enemy's Identification Friend or Foe (IFF). MoEs for this are shown in Figure 4.8.

Armed forces use a number of means of IFF: radio transponders on aircraft, uniforms, recognition symbols on vehicles. They also use procedural methods for deconfliction. Network-centricity should help there, because of better dissemination of information about where different units are supposed to have troops - but only if the equipment and software are right. The use of paper messages now seems very old fashioned – however for guerrillas it has the advantage of not using radio frequencies that are probably monitored by their opponents.[1]

[1] The communist terrorists in Rhodesia in the 1970s used paper communications.

IFF can be mimicked by the enemy.[1] There is also the threat that the enemy will activate our IFF, it assist him target our assets. It was for the latter reason that RAF Bomber Command aircraft in World War II used to switch off their IFF on leaving UK controlled airspace.

There are also reliability issues with IFF. This was one of the reasons for US fighters in the Vietnam War had restrictive RoE, which required visual recognition (which greatly handicapped their use of radar-guided air-to-air missiles).

4.8 Degrade Enemy Systems

The objective of degrading enemy systems is to make them work less well. This can be a useful by-product of another form of attack. If systems do not work very well, the users have less confidence in them, and act accordingly. Figure 4.9 shows MoEs for this.

Methods of degrading enemy systems include:

- *Swamping*. Sensors are provided with large numbers of false targets. Communication systems are filled with messages that people do not have to read, but which absorb time and make it difficult to find the messages that matter.

- *Jamming*. This makes it difficult to use radio-frequency sensors and communications – though anti-jamming techniques may counter it.

- *Courier interception*. If people are sending information by courier, then the interception of some couriers will degrade trust in couriers. In recent history, air tasking orders have had to be flown to aircraft carriers because incompatible software made electronic transmission impossible.

- *Cutting cables* (see Section 3.3.8)

- *Targeting those who use system* (see Section 3.3.8)

[1] See Section 3.3.5. This mentions the use of German troops in US uniforms during the Battle of the Bulge in December 1944. It also mentions pseudo-terrorists, who mimic terrorists to infiltrate terrorist gangs and gain information.

		Target Behaviour						
	Colour Coding	Enemy increased friction	Enemy makes less good use of information	Enemy misses opportunities to strike back	Enemy restricted in communication use	Enemy transmits larger numbers of verification messages	Enemy has increased levels of friendly fire	**Consequence**
1								Failure
2		TRUE	TRUE					Limited success
3		TRUE	TRUE		TRUE	TRUE		Limited success
4		TRUE	TRUE				TRUE	Limited success
5		TRUE	TRUE		TRUE	TRUE	TRUE	Limited success
6		TRUE		TRUE				Success
7		TRUE	TRUE	TRUE				Success
8		TRUE		TRUE	TRUE	TRUE		Success
9		TRUE	TRUE	TRUE	TRUE	TRUE		Success
10		TRUE		TRUE			TRUE	Success
11		TRUE	TRUE	TRUE			TRUE	Success
12		TRUE		TRUE	TRUE	TRUE	TRUE	Success
13		TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	Success

Figure 4.9 MoEs for Trust Attack to Degrade Enemy Systems.

5 Conclusions

- Trust is an area where there are no universally agreed definitions. There are a range of meanings for some of the terms used. (Sections 1 and 2.)

- Some of the people doing research on trust are presenting as new research things that have been understood for over a hundred years. However they are presenting it in trust jargon, so it looks new. (Section 3.1.3.)

- The use of real-life (usually historical) examples provides a level of validation. Sometimes they show that apparently appealing ideas are not true. (Section1.2.4.)

- It is not obvious that influence diagrams are the right way to model trust. They are useful for sketching out influences, and for understanding what other people think are key influences. Traditional software techniques are a more naturalistic way of modelling trust. (The section of the full report containing influence diagrams is not reproduced in this paper.)

- The measures of effectiveness used (in Section 4) caused significant (and to the author unexpected) debate:

    - People who are used to models tend to pick measures that models can easily produce. Some of these are not available in real operations (at least not accurately). Such measures are often attrition-based in thinking. Attrition-based measures are not necessarily monotonic in Effects Based Operations.

    - The measures of effectiveness presented in this report are based on the effects people are trying to achieve. They are based on things that are knowable at the time. They have taken the form of a series of booleans.

    - In information operations, we have to bear in mind that the enemy may be conducting information operations against us. Sometimes we have to attach a health warning to apparent success.