Click here to view PowerPoint presentation; Press Esc to exit

A System Shock Approach to Modelling Clandestine Network Disruption

Mr Tamlan Dipper
34a Dorset Square
London
NW1 7QJ

induna@talk21.com

SUMMARY

Clandestine networks, in their most infamous form taking the guise of terrorist groups, are a clear danger to the stability and well-being of society. Without trying to contradict other approaches or reinvent the wheel of counter-terrorism, a theoretical basis of system shock was chosen in the formation of a model to support counter-terrorist initiatives. This model took as its focus the disruption of successful terrorist operations. In doing so it drew upon operational art, group behavioural studies, and psychological research into problem solving. The result was a model of operations as a 'concert' of properties being activated to produce an environmental change. Damage to the properties, or the ways they were included and activated as part of the concert, lead to the infliction of system shock upon the operational whole. Ineffective operations rendered the whole target system ineffective. Procedures for applying this model in different circumstances were examined, and experimental exercises performed to verify usability by non-specialists. The conclusion of the study was that, while more work was needed to refine this approach, it showed promise, and reinforced the notion that terrorists are not an invincible adversary.

1. INTRODUCTION

It can be of no news to any reader that we have entered a new phase of the global threat from terrorism. A phase characterised by greater professionalism, resourcefulness, and ruthlessness. Significant numbers of opponents are eschewing serious negotiation, and are instead fixated upon world revolutionary and even apocalyptic goals. For this reason several authorities, including the head of Britain's Security Service [Mannigham-Buller 2003] have specified a need for disruption of terrorist activities.

1.1 Aim of work

To support existing counter-terrorist efforts by the creation of a model and supporting procedures that focus on clandestine network disruption.

1.2 Clandestine

Clandestine, as an adjective, refers to a thing secretive or hidden in nature. However, there are two potential interpretations of the phrase "clandestine network disruption" in the title of this work. One interpretation suggests it is the disruption that is clandestine. The other interpretation suggests that it is the network that is clandestine, and to be disrupted. Both interpretations are, hopefully, valid in the context of this work.

The need for clandestine disruption is specified in section 4.2. The need for disruption of clandestine groups in the counter-terrorist context may be derived from the fact that terrorist groups and activity are *defined* by their clandestine character.

Paper presented at the RTO SCI Symposium on "Systems, Concepts and Integration (SCI) Methods and Technologies for Defence Against Terrorism," held in London, United Kingdom, 25-27 October 2004, and published in RTO-MP-SCI-158.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **25 OCT 2004**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **A System Shock Approach to Modelling Clandestine Network Disruption**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Royal Military College of Science, United Kingdom 34a Dorset Square London NW1 7QJ**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

See also ADM201977, Systems, Concepts and Integration Methods and Technologies for Defence against Terrorism (Systemes, concepts, methodes d'integration et technologies pour la luttre contre le terrorisme)., The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**36**	

The logic underlying this point may be stated briefly as follows. That is, where a party has opted to use force, but is possessed of inferior military strength, they will be forced to keep their membership and actions clandestine. Doing so avoids negative sanctions executed by the defender. With the emphasis on remaining clandestine, the group will be unable to support or sustain operations that require large quantities of men and materiel. Combining the clandestine imperative with the aforementioned lack of military force, we can see how only very lightly defended targets will be chosen for attack. Thus we see how and why terrorists prioritise civilian and off-guard military assets.

This is one reason why the clandestine characteristic was chosen rather than the title 'terrorist'. The second, related reason is that other definitions can be so difficult to apply across the range of groups definable as terrorist, taking in as they do organised criminal and cult-like attributes.

2. FROM THEORY TO MODEL

Decision making is a fundamental process for any organism or organisation. In attempting to reach decisions it can be said that there are three steps.

- The user (organism or organisation) must choose the objective function of the exercise. That is, what they are hoping to achieve.
- The user then adopts a modelling technique to formulate the problem in hand.
- The user evaluates any proposed solutions by fitting them against the model and comparing their performance using the objective function.

The first and second stages of choosing an objective function and creating a model to achieve optimality in the objective directly inter-relate. This is via the process of abstraction which transforms the manifold and almost infinitely complex reality into a useful form.

Law and Kelton [Law & Kelton 2000] demonstrates that there are a number of classes of model that range from the mental to the mathematical. These cover an increasing level of abstraction from reality as they increase in simplicity. Clearly, as the models become more abstracted there is the potential for them to represent the facts more poorly, resulting in a correspondingly poor judgement.

Coping with what factors to include and what to exclude is usually covered by the acceptance of a particular theoretical standpoint. In a business problem we may feel that the correct objective function is cost or profit. Choosing this leads us to seek a model which can represent the factors known to impact most significantly upon the cost [Taha 1997]. As an alternative, if we had chosen a standpoint of lowest risk this might lead to the examination of other factors in turn such as prevailing weather conditions. The choice of the objective function may be almost entirely subjective, but once it is done the success or failure of any abstraction is more objectively measurable.

2.1 Seeking an objective function

In the foundation research for this work a number of theories regarding conflict, counter-terrorism, and counter-insurgency were looked at. These included: attrition; intimidation; law enforcement; logistic interdiction; social network analysis (SNA); negotiation; and psychological confrontation.

Each was considered in terms of its proven record of successes, and the utility is presented as a foundation for modelling support. Conclusions regarding these are shown below, the list of positive points being:

- Attrition correctly establishes that total elimination of terrorist men and material should result in severe disruption.

- Intimidation, negotiation, and confrontation analysis highlight the importance of the psychology component.
- Law Enforcement showed the critical importance of working within the law and the efficiency of targeting only guilty parties.
- Logistics based disruption correctly establishes the importance of support in terrorist operations.
- SNA shows the importance of agents in the terrorist network and links between them.

On the other hand, we also observed the following negative points.

- Attrition, intimidation, and law-enforcement models all fail to provide means of efficiently achieving the goal of disruption.
- The logistics based approach does not include details of how the need for logistic support arises, through attrition, accident, and use.
- SNA did not show sufficient sophistication in dealing with the bonds that make up a terrorist network. Nor did it show how the network carries out activity in any way that would help targeting those activities for disruption.
- Negotiation and psychological confrontation showed insufficient focus on forcing disruption upon the target network.
- None of the models coped very well with missing information.

2.2 System Shock as an Objective Function

In the end a completely different objective function was chosen. One that seemed to permit both modelling support, and acceptance of the strengths of the aforementioned approaches. This objective was ‘system shock’.

System shock is a concept originating in Soviet Russia, after the First World War in the writings of (among others) Marshal Mikhail Tukhachevskii. His aim was the rejection of an attritional mode of warfare, that took as its focus the piecemeal annihilation of an opponent. His replacement notion was the inducement of a state in the opponent where he was unable to act as a result of damage inflicted to every level of his organisation, including front line units, intelligence, logistics, and even the mind of the commander – ‘udar’. This inability to act could then be used as the victor chose to impose their will on the defeated, whether through annihilation or political domination.

The elaboration of this earlier concept with modern systems theory has given rise to an increasing body of work on ‘system shock’, much of which is described by Shimon Naveh in his 1997 book ‘In Pursuit of Military Excellence’ [Naveh 1997]. Here a continuum within a system is laid out, extending from the strategic vision, through a sequence of operations, executed by a range of tactical activity. A strategic vision is an idealised world view. Operations are events which result in an output that represents a change to the environment. Tactical activity represents the striking of matches, speaking of words, and climbing ladders that is necessary for an operation to be effected. Shock is defined as a state wherein the system’s tactical activity is no-longer oriented upon its strategic vision.

This state of shock can occur by failure at any one of the three points: strategic, operational, or tactical. Muddled, confused, or conflicting strategic visions in an organisation induce shock [Zander 1968]. Operations whose output does not bring the strategic vision closer induce shock. Tactical activity that is frustrated by intervention, chance, or is unsuccessful also induce shock.

A choice then had to be made as to which level or levels we might seek to model. The strategic level was felt to be a product of forces that lay almost beyond the scope of intervention, and was therefore inappropriate in this context. The tactical level, by contrast, was not only within the scope of intervention, but already the subject of a wealth of expertise in the police and armed forces, suggesting it could be a less fruitful avenue to pursue. On the other hand, the operational level was felt to be both capable of abstract definition, and lacking in modelling support.

2.3 Observations on operations

A large number of sources in the military science, systems engineering, and psychological fields, were used to build a picture of operations. The intention was to encompass anything from grand operations such as an armoured turning manoeuvres, right through the execution of a car-bombing, to purchasing a newspaper. These observations may be summarised below.

- Operations fail through accident, poor planning, poor execution, and intervention. Even terrorist operations fail, such as the Al Qaeda attack on USS *The Sullivans*, where the attack boat sank under the weight of its own explosives.
- Failures can often be traced to consistent factors across different incidents; Successes likewise.
- Psychological factors could be as important as material factors.
- Operations could be, and often were, revitalised following failure, given certain behaviours were followed.
- Individuals often occupied highly specialised roles within operations, the disappearance of whom could be catastrophic unless another individual could assume that role.
- The mental models humans use in the solution of problems – mounting operations – seemed to be re-used in later problem-solving.
- It might be helpful to generate a bespoke characterisation of the building blocks which make up an operation.

3. MODELLING OPERATIONS FOR INFLICTING SYSTEM SHOCK

We have therefore decided upon an objective function and theoretical standpoint from which to pursue our objective: system shock. We have also reached some conclusions about the nature of operations. Based on these it seemed possible to reach a useable characterisation.

3.1 Basics – Elements

We are quite used to describing operations in terms of physical objects and events. These could be a bomb, a delivery, or an explosion. In the example in Figure 1 below, we are concerned with an AK 47 assault rifle as an element. Objects or events are described here as elements. In the context of a specific and unique operational plan the elements involved will be uniquely identifiable.

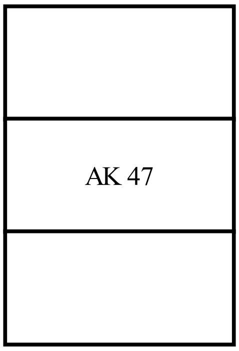


Figure 1: An element

The example in Figure 1 shows a single element, but it may be expedient to represent several identical elements by the addition of an asterisk (*) outside the box. However, this shorthand should be avoided where time exists to elaborate more comprehensively, with each element being shown individually.

3.2 Basics – Properties

One of the conclusions reached during this work was that a more utilitarian architecture for operations could be reached by looking at the properties which made them up. Every element has a nearly infinite set of potential properties which it may possess in varying degrees.

Very basic low level properties are the easiest to consider, and would be represented by weight, temperature, velocity, and so on. However, it may be equally important to consider higher level properties such as fear, leadership, and force inequality. In the example below our rifle is expressing the property of ‘deadly force’.

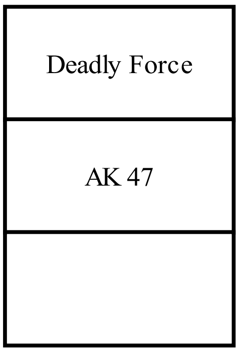


Figure 2: An Element and Property

A qualifying attribute of properties is that any element can be said to possess the property even if the degree of the property is ‘zero’. For example, an assault rifle, a broadsword, and a teddy bear can express the property of deadly force in varying degrees. Conversely, all three can also express the property of ‘innocuous’ on an inverse scale.

3.3 Basics – Conductors

Elements do not express all properties all the time, nor do they always express them in the context of a specific operation. For them to do so some sort of agent is required. The agent’s role is to cause the element to express the correct property in a harmonious fashion with other properties making up a specific operation. This implication of harmonious and timely coordination gives rise to the name: conductor.

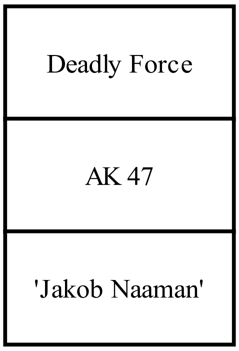


Figure 3: An Element, Property, and Conductor

In the above example a fictional character, 'Jakob Naaman' is conducting the property of deadly force in the rifle. This activity is an operation in its own right, and the result of a wholly separate set of properties that are in action. We will return to an example of this at the end of this section. Suffice to say for the moment that what properties are in action are best left to the user to define appropriate to their modelling purpose.

3.4 The Operational Focus

We have already seen that the operation may be characterised as an event which results in a change to the environment. The name, and sometimes description, of the event is shown in the 'operational focus' for the operation. The operational focus also contains the 'grand conductor' whose role is that of a normal conductor, but additionally being responsible for the link the operation has to the strategic vision.

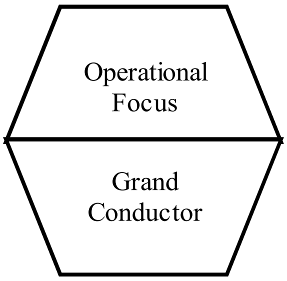


Figure 4: Operational Focus & Grand Conductor

In general, when defining the operational focus it is best to think in terms of how the world will appear when the operation is complete. Therefore, while 'Shooting the Prime-Minister' is an acceptable working title, 'Dead Prime-Minister' is more useful. The tools the user envisages in action can be worked into the model beneath the operational focus.

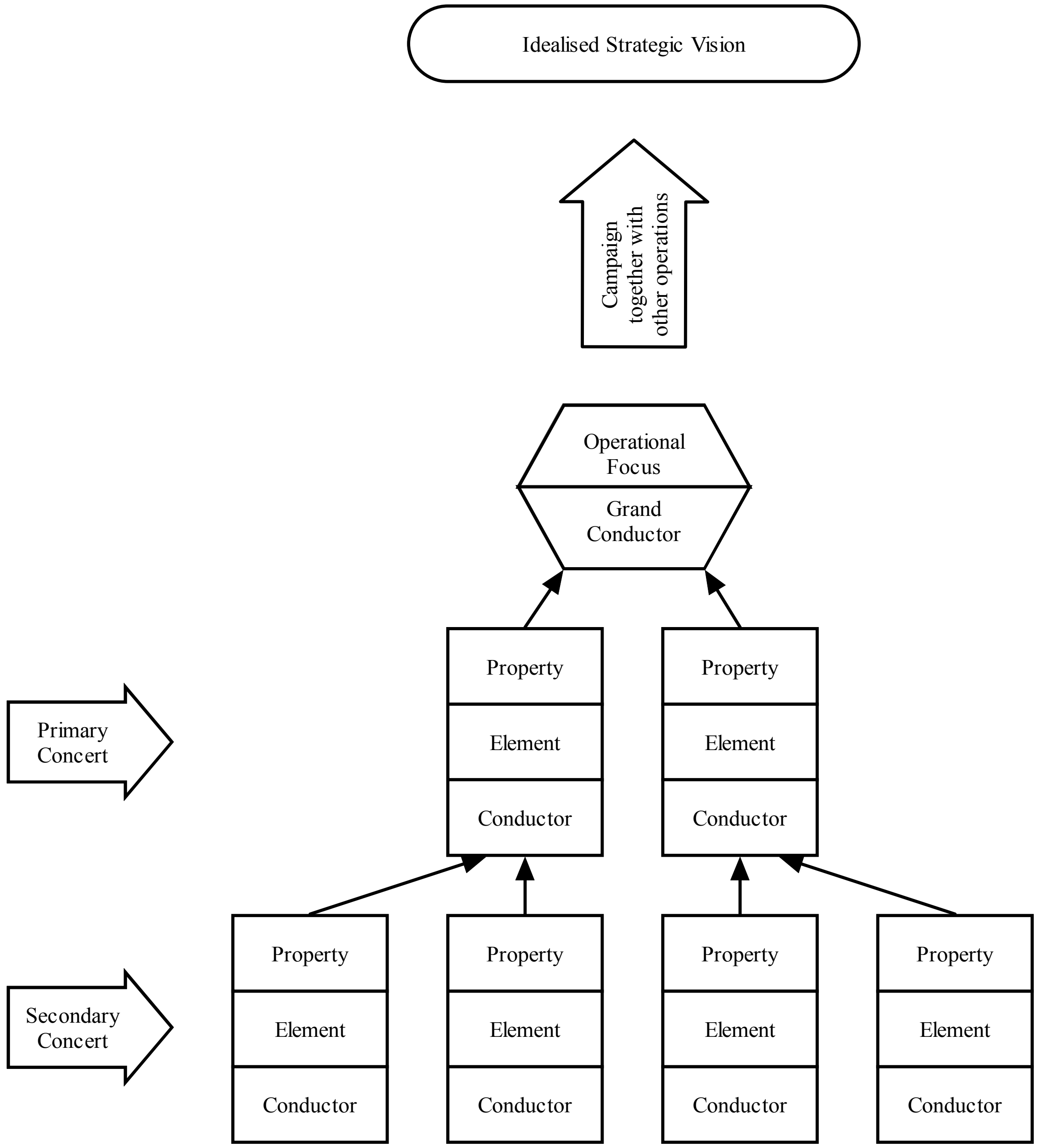


Figure 5: Generalised Operational Concert

Shown above is a generalised version of the operation, including the upwards link. We use the term ‘concert’ to remind the user that issues of timeliness and harmony are implicit through the effective action of the conductors.

3.5 Criticality and System Shock

We can see, then, how each of the property-element-conductor triads is appears in the model. What we have not yet discussed is the essence of system shock that they can represent.

When building the model of an operation the focus is predominantly on properties. Certainly properties only arise, given an element and conductor, but it is the properties that combine to produce the desired effect.

It is damage to the properties that make up an operational concert which send it into shock, not a vague notion of damage to elements or conductors. This is important to the creation of the model, and the effectiveness of the conclusions drawn from it, but it has two other benefits. Defining in terms of properties not elements or conductors allows us to perceive possible permutations in the concert, the process of which we will return to in the analytical procedure. The second benefit is that it gives us increased flexibility in terms of proposing our own operations to damage those properties since we are no-longer fixated upon material destruction, or things that can be materially destroyed.

3.6 Recovery from System Shock

It is an unfortunate fact of counter-terrorist activity that damage done today is healed tomorrow. It was therefore considered vital to the creation of an appropriate model that the chosen approach could represent this. Specifically it should assist the user in predicting both the longevity of effect, and if possible, the nature of the response.

In this approach the ‘ideal’ procedure is as follows:

- Damage occurs to a critical property.
- A friendly agent, almost always the conductor for that property, appreciates that the damage has occurred.
- The agent will usually try to reassert the appropriate level of the property
- While he does so he will communicate to his conducting superior that his property is damaged, and allow the conductor to refer upwards to the focal conductor who will halt the remains of the operation until the problem is resolved.
- Typically, if the local conductor is unable to reassert the property he will refer to his superiors. They will then begin to attempt reassertion of the damaged property. This is because damage to the inferior property is communicated instantly up the chain of properties to the focus. However, they may also act in anticipation as they realise their own properties are damaged.

Reassertion of a damaged property occurs in one of three ways. The first is through analysing the source of the problem and eliminating it. This can be physical repair or neutralisation of the hostile agent who is causing the problem, and is the most obvious. The second more subtle method is to replace the element that is providing the property. An example of this would be the use by the 9/11 hijackers of knifes to ‘intimidate’ the passengers on the aeroplanes instead of more traditional firearms or explosives, that airport security would have prevented from getting aboard the flight.

The third, and far more subtle method is to allow the operation as a whole to mutate. The way in which this occurs is characterised by compensating for a weaker property at one point with a stronger property at another. For example, an effective car bombing requires proximity relative to a given explosive force. We can see that reducing either explosive force or proximity to zero will render the operation as a whole unsuccessful, so on the understanding that the terrorists are believed to possess around 100 kgs of ammonium phosphate explosive, we position the requisite security cordon around potential targets, damaging the proximity property in their concert. Perceiving the security cordon has done this damage, a mutation would be to increase the size of the explosive charge so that it can again cause the required damage from the given proximity.

Needless to say, recovery is not always a given, quick, or easy, for the target. Ways in which recovery can be made a good deal harder are discussed in section 4.

3.7 Example Operational Concert – The Conductor Concert

In order to provide an example and to elaborate further on the notion of what constitutes a conductor it has been decided to provide one interpretation here.

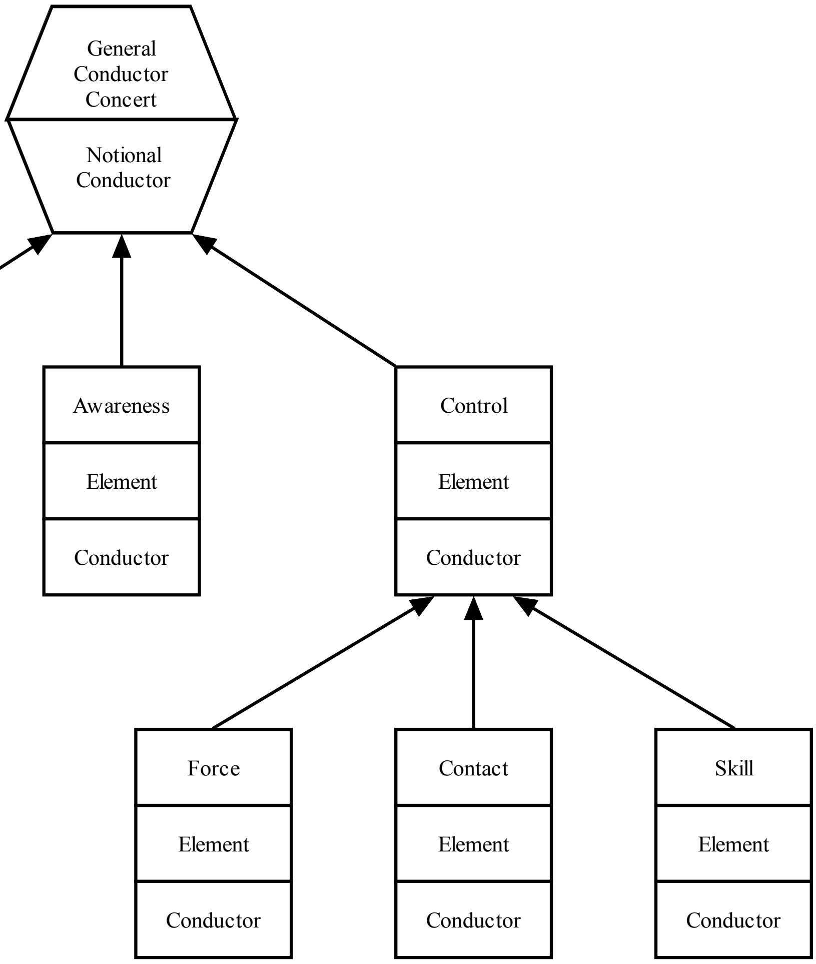


Figure 6: Generalised conductor concert

Shown above is a hypothetical concert derived from observations made through the work and discussion with colleagues. Users are welcome to develop their own operational concerts derived from their expertise, however. Indeed, users may feel it is not necessary to elaborate to this degree. As always needs and circumstance govern the procedure.

In any event, an explanation of the above model may be helpful as an illustration of the overall model structure. We begin with the ‘awareness’ property. This is derived from Gibson’s [Gibson 1978] notion of awareness, reflecting the understanding an individual has that an object possesses a certain usefulness to them. Here it means simply that the individual has to know that they need to activate the property in the element. If they are the conductor of the focus the property is feeding into then the awareness is derived from themselves as conductor in a loop. The element that gives rise to the awareness is the example they are following, which can be internal or external. Knowing about a previous operation where the element was used for the same purpose will provide this. Without the awareness property the element can be in possession of the property but rest unused. Prior to the imaginative leap that lead to the events of September 11th, few were aware of the deadly force property that a terrorist operative could harness in a passenger jet.

‘Motivation’ is the willingness to participate in the operation. The element is defined as an intrinsic or extrinsic source. Intrinsic source means that the individual is personally in approval of the operation; a characteristic of many jihadi terrorists, even where the operational focus involves mass destruction. But equally, even jihadis and other cults utilise operatives whose motivations arise from such things as social inclusion, cash, or the threat of violence. The conductor of such a property is rarely the individual themselves, but typically a mentor, unit leader, or cleric. One noteworthy aspect of this is that intrinsic motivation to participate in a given operation will be damaged by failure and system shock [Zander 1968] although that may be fixed under a new more promising leader, or by switching to an external motivator.

The final property in our conductor concert is ‘control’. This has been elaborated into three secondary properties; noting that secondary does not in any way imply that they are of secondary importance. The loss of any of these will cause the control property to fail and inflict system shock on the concert as a whole. This in turn will inflict shock on whichever concert the conductor property is involved in.

The first property in the control concert is ‘force’. The nature of the force refers to method by which the element the conductor is using is activated in its expression of its critical property. This can be physical, intellectual or moral force depending on the element, and can arise from elements such as a rank, a historical event, the body, hands, and so on. The conductor is almost always the individual themselves although it is possible to imagine external sources activating the element as a force. For example, the immense media interest in Osama bin Laden has ‘activated’ his past exploits from the Afghan war and given him credible force over many disparate human elements.

The second property in the control concert is ‘contact’. This property refers to the fact that the conductor must be able to apply the force generated. this can arise from elements such as mobile phones, radio controls, and even books and letters, depending on the context. Once again, it is rare that the conductor is anyone other than the individual themselves.

The third property in our control concert is the ‘skill’ of activating the property in the element. This obviously of key importance and refers to the procedural knowledge and capacity to intelligently govern the procedure in hand. The element that gives rise to it is the agent’s body/brain. The conductor in this case will be as before either the individual or the superior depending on whether the skill is already present or has yet to be imparted. Without the relevant skill no amount of contact and force will be of any use.

Note that if there are several different types of contact or force required in the activation of the concert by the conductor then each should represented as its own property in the model. For example, to contact each element the a conductor may need to command both distant and direct communication properties. Each of which should be represented as its own triad.

So it is that we can see the way in which an operational focus on conducting some other property can be broken down into its respective components.

4. USING THE MODEL TO INFLICT SYSTEM SHOCK

The purpose of describing operations in this way was to assist the inlfiction of system shock at the operational level. With this in mind, some guidelines for use have been produced. However, the user is very welcome to adapt and develop their own.

The simplest approach for building the model is:

- Gather subject area experts and end users

- Define operational focus
- Hypothesise concert consisting of just properties, leaving blank spaces for elements and conductors

Further action depends on the interest of the user. It is important to note, however, that in the course of any use of the model, most groups of users will generate new understandings of the problem. Therefore, as a general note it is vital to permit wholesale scrapping and reformulation of the model under consideration, as time goes by.

4.1 Inflicting system shock on a specific operation

In its simplest form, system shock consists of damage to a critical property. However, there are a number of routes to attacking the concert that the model should reveal.

The ideal position to be in is to know all three components of a property-element-conductor triad. However, what is far more common when dealing with a clandestine network is that neither the element nor conductor is known in a specific triad. Instead, it is simply the case that the users have been able to hypothesise critical properties, using historical examples and subject area expertise. In a situation where the element and conductor are known but not the property we are likely to be facing a specific threat capability analysis rather than trying to cope with a specific operational concert, since knowing what the operation is should certainly permit us to establish what property the element and conductor are there to express.

Knowing only the property gives rise to three options. Firstly, since we are of the opinion that the property is critical to the operation, we may consider improving detection and sensing of the property in relation to certain targets. These sensors may be mechanical or human, guiding the briefing of security details. Secondly, we may be of the opinion that requisite levels of the property concerned are only present in a few elements. Where this is the case we may initiate surveillance of these elements. An example of this may be the apparent concern the British police show over thefts of mechanical earth-moving equipment, following their use by the IRA, due to their unusual robustness in delivering explosive devices. A third option is to cap the potential levels of a property in a given context. An example of this would be to pedestrianise an area surrounding a vulnerable target, and/or fit barriers to vehicles above a certain size. This measure will cap the size and weight of any explosive device that can approach (making no mention of the adaptive response this particular example would trigger).

If we know the conductor for an element for whatever reason, we may target them by elaborating the conductor concert they will require, and treating that concert in the same way we are dealing with the operational concert.

If we know the element that the target group is going to be using, or would like to consider a specific element for any reason, we must seek to prevent the element from expressing the requisite property. This can be through attacking its conductor, as seen above, or through attacking the element itself. If no obvious routes are apparent, the user can elaborate the concert giving rise to the property and look at inflicting damage to one of these properties, knowing that the loss of one of these will cause damage to the property they were originally considering.

4.2 Preventing Recovery

The procedure outlined in 4.1 is acceptable as an initial step in considering what must be done to inflict system shock. However, as previously noted, operations are not static, and recovery should always be considered even if the user does so without the aid of formal modelling. Should they wish to model recovery formally the user should consider the recovery process described in section 3.6 as the ideal.

One approach on the part of the user is to take this as an ideal which they are seeking to disrupt. The most obvious route to doing so will be the infliction of damage to the operational concert brought into play by the terrorists to enact one of the three recovery options that they possess: repair, replacement, or mutation.

The second approach the user may follow is to prevent recovery from taking place by stopping the target realising damage has occurred. This can be achieved through clandestine action against either the property in question, or through clandestine severing of communications between the property's conductor and the other conductors in the operation, particularly the superior conductors. In either event, the result of successful clandestine disruption should be that the operation wil be enacted only to fail catastrophically – that is, the successful actions elsewhere in the concert will be to no avail, even exposing further vulnerabilities.

The third approach to recovery is to actually exploit the recovery process to damage the operation. If the recovery process can be triggered there are two concomitant negative impacts. The first of these is that recovery takes time, the second is that a replaced or repaired element will have usually possess an uncertain degree of the desired property. Sometimes the new level will be superior, but much more frequently the new level will be worse, at least initially.

Triggering the recovery process needlessly can occur in two ways identified so far. The user can make the target recover in anticipation of damage, as terrorists do when they believe a member of an active cell has been taken for questioning, or when they believe communications are compromised. The second more difficult way is to manipulate their perceptions of properties in the concert, in particular the status of targets and state capabilities in detection and resilience. However, while such attempts have been made in the past under conditions of war [Howard 1990] with considerable success, doing so in peacetime would bring its own complexities.

Provoking recovery of any kind, necessary or unnecessary, will force activity on the part of the targeted network. This may help officers maintaining surveillance of a group to identify individuals higher up in the hierarchy, if local terrorist operatives are unable or unwilling to resolve a specific issue.

4.3 Threat Assessments Using the Model

One other use that the model may be said to possess is that of aiding a threat assessment for a given group. This is a corollary, to an extent, of the ability the model has to show when any operational concert is infeasible due to damage.

For a threat assessment to take place the user must first stipulate what operations constitute the threat they are concerned by. In certain circumstances we may not feel significantly threatened by small scale attacks, but be interested in whether the subject possesses the ability to execute the detonation of a dirty bomb over our capital city. In such circumstances the procedure is as follows.

- Construct or re-use a model of the operational threat, showing only the properties required, leaving spaces for the elements and conductors.
- Using known and speculative information, attempt to 'fill in the blanks'
- Highlight areas where information is deficient
- Highlight properties which the group cannot currently generate, but which should be flagged for immediate attention if they appear to be seeking to acquire the missing element or conductor.

In this way the user can state what the group is capable given the current knowledge. The user can also state what operations the subject network may be plausibly capable of. Moreover the user can specify areas of interest for further investigation, and flag future developments for action.

5. TESTING OF THE MODEL

Clearly, application of this model in service can only occur after some trial use. However, realistic trials were impossible to arrange up to this point, and only basic validation has been possible.

5.1 Usability

The first type of validation has been the application of the model and procedures to 'mock' problems, using staff and students at the Royal Military College of Science, to test whether how difficult it was to understand and use. Feedback from these individuals described the approach as helpful and easy to use, particularly the focus on properties, as a way of building hypothetical operational concerts. Negative feedback stated that some practice was initially required to grasp the new concepts, but all test subjects stated that they had not used any better method to approach the problem.

5.2 Historical Case Study

The second type of validation was the mapping of an historical case study using the model. The case chosen was that of a terrorist group from the United States, called the 'Weather Underground Organisation' (WUO), or 'Weathermen'. They were selected as an example of a terrorist group that had run its course, from birth to death (1969-1976/1981), and had been quite well described by open sources, including declassified Federal Bureau of Investigations files.

What the case study showed was that the group obeyed the principles set out above. They had an avowed 'Strategic Vision' of being "against everything good and decent in honky America", articulated by a series of operations. Importantly, the architecture of the operations remained almost stable in terms of properties. This can be demonstrated in Figures 7 and 8 below.

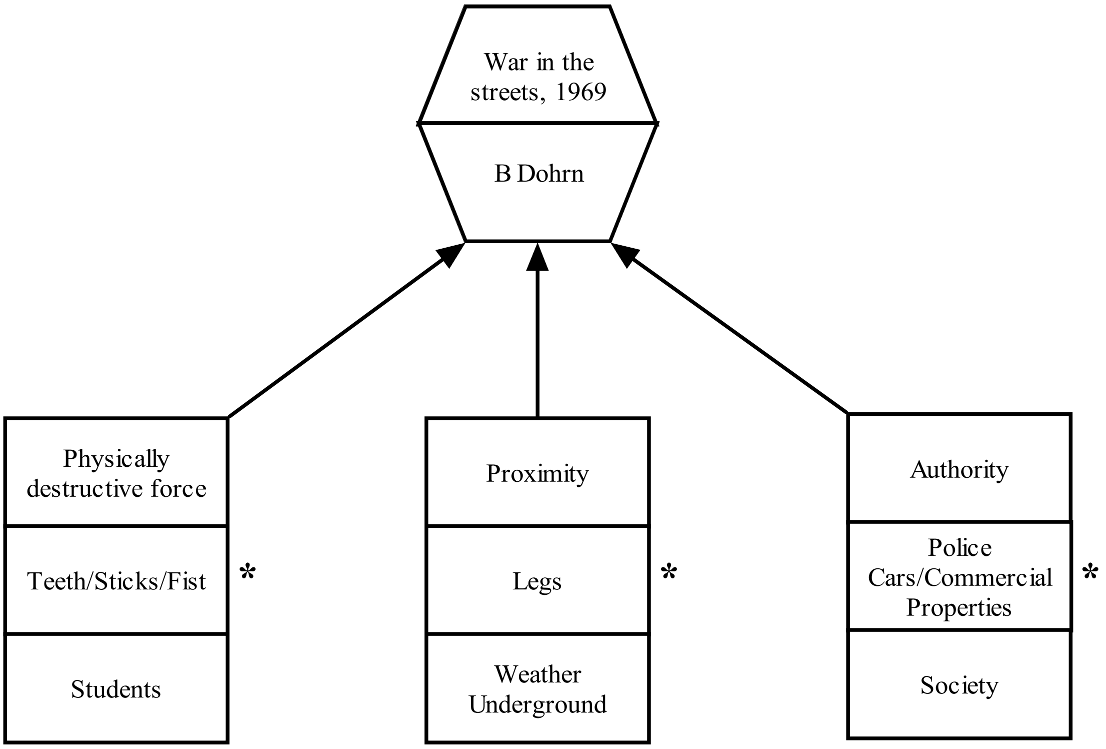


Figure 7: Model of the war in the streets caused during the Days of Rage

The operation in Figure 7 above was the first organised by the group, and represented an attempt to bring violence home to downtown America, supposedly in protest at the Vietnam war.

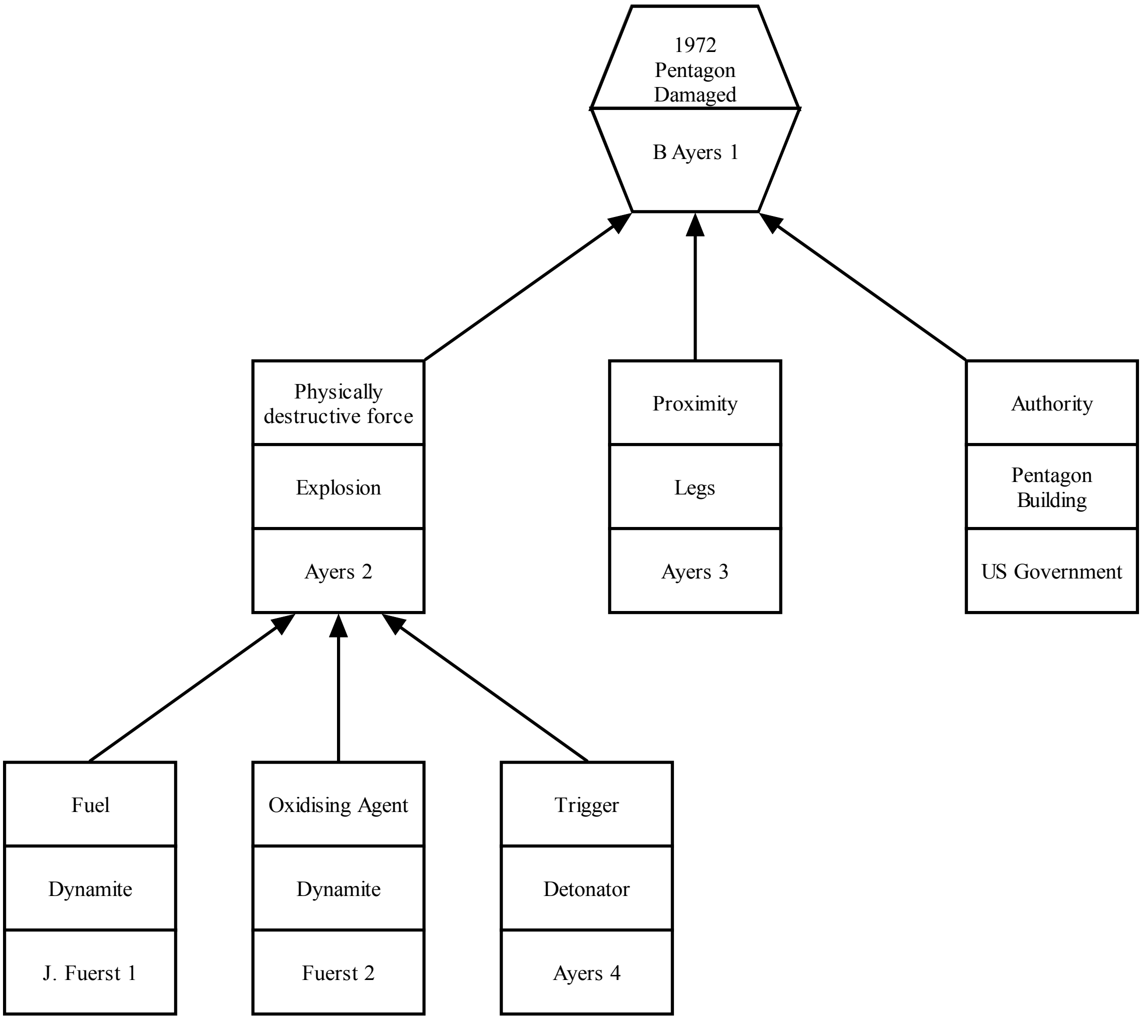


Figure 8: example operation typical for later actions

If we take a later operation mounted by the group, as shown in Figure 8, we can see how the essential structure at the level of the primary concert remains similar to the earlier Days of Rage. However, the group has sought to increase the level of physically destructive force by replacing crude implements with an explosive device.

Another important observation was that the model permitted elaboration of the role within the group's operations being played by external groups, particularly a Cuban/KGB connection, and the North Vietnamese Government. The example in Figure 9 is of Ted Gold operating as the Grand Conductor of bomb-making and bomb-detonating operations.

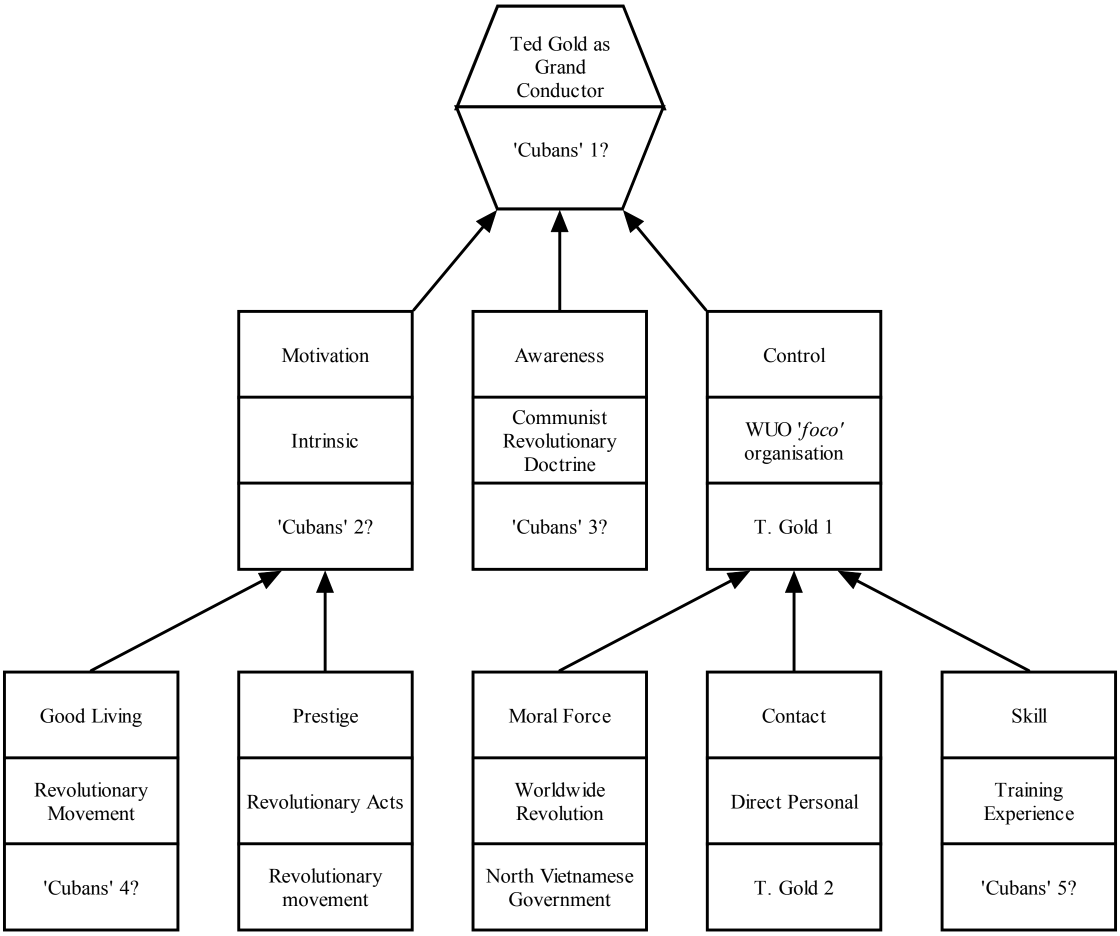


Figure 9: Example of Ted Gold as Grand Conductor

Initially difficulties arose over time, since the group was losing conductors and material resources to police action and accidents, yet they persisted in operational capability. However, shifting focus to recovery easily explained their capacity to continue acting. The acquisition of replacement materials was effected with the aid of Cuban money and false documentation, guns and explosives being freely available in the United States, while the conductor concerts, most of which were similar to that shown in Figure 9, functioned because of continued Cuban and Vietnamese involvement. These countries being profoundly concerned with American commitment to the South Vietnamese government, and the general principle of American intervention in foreign communist countries.

The criticality of the external link was amply demonstrated with the sudden cessation of activity following 1976 – 1975 marking the end of hostilities in Vietnam. Neither Cuba nor Vietnam had any further interest in supporting further terrorist activity, and appeared to cut all ties. The loss of these parties as conductors and the loss of the resources they supplied as elements for operational concerts easily explains the drop-off in WUO activity, and the divisions they suffered subsequently.

The period 1976-1981 was characterised by attempts at recovery on the part of leading figures such as Bill Ayers and Bernadine Dohr, trying to re-assert control over operatives, acquire prestige, and generate cash for materials and simple living expenses. None of the attempts made were noticeably successful, with the final act being an attempted armoured car heist in New York state in 1981, that went badly wrong. This failed heist, which was also explicable using the model, lead to the incarceration and surveillance of all remaining members.

Overall, then, the model seemed capable of being used, understood, and fitted to real world examples.

6. CONCLUSION AND RECOMMENDATIONS

Disruption of clandestine networks is a far from simple problem, the solution to which will owe far more to the work of the security services than to modelling. However, it is a cornerstone of this work that such work will be easier with the support of clear, theoretically sound, useable models. The creation of such models will be a long and iterative process, and this may be just beginning. For this reason I feel that the principles underlying this work are as important as the model chosen to express them.

- Any approach must be able to cope with partial information
- The chosen objective function must be flexible enough to work within the law, and to consider less-than-lethal interventions to cause serious effects
- Damage, and recovery from damage, are two halves of a single whole
- Frustration of the enemy's activity will result in frustration of the enemy's structure, purpose, morale, and ultimately their very existence

In addition to these principles I feel that the work has lent credence to the notion that System Shock represents an excellent theoretical objective function for counter-terrorist disruptive planning.

Given the lack of realistic trials of the ability of model to support actual disruption it is difficult to make any confident assertions about its validity. However, it is certainly my hope that opportunities will arise for further testing, and revision of the model and its supporting procedures.

7. REFERENCES

[Gibson 1978] J.J. Gibson, "The Ecological Approach to Visual Perception", Lawrence Erlbaum Associates, 1978

[Howard 1990] M. Howard, "British Intelligence: Vol. 5, strategic deception"; HMSO, London, 1990

[Law & Kelton 2000] A.M. Law, D.W. Kelton, "Simulation, Modelling, & Analysis" 3rd ed., McGraw Hill, 2000

[Mannigham-Buller 2003] E. Mannigham-Buller, "Global Terrorism – Are we meeting the challenge?", James Smart Memorial Lecture, 2003

[Naveh 1997] S. Naveh, "In Pursuit of Military Excellence: the evolution of operational theory", Frank Cass, 1997

[Taha 1997] H.A. Taha, "Operations Research: An introduction", 6th ed., Prentice Hall

[Zander 1968] A. Zander, "Group Dynamics: Research and Theory", 3rd ed, Harper & Bros, 1968

A System Shock Approach to Modelling Clandestine Network Disruption

Tamlan Dipper

Royal Military College of Science,

United Kingdom

What and why

- Modelling support for counter-terrorist activity.
- Focussed on disruption as most urgent need
- Clandestine in both targets and methods
- Mainly based on work carried out with the Royal Military College of Science, Shrivenham, UK

From theory to model

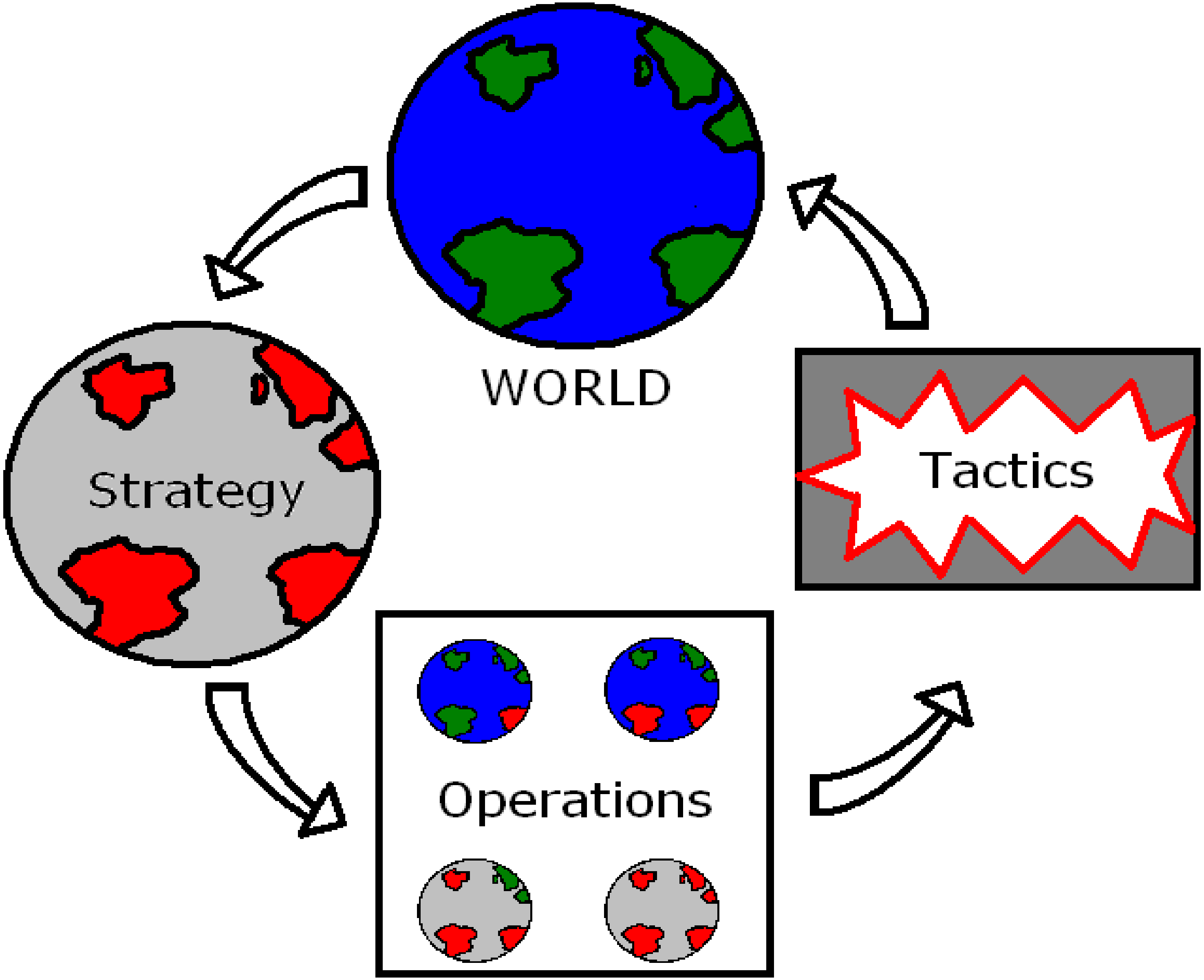
- Needed foundation for work
- During research looked at some existing approaches
  - Attrition
  - Intimidation
  - Law-enforcement
  - Logistics Interdiction
  - Social Network Analysis
  - Negotiation
  - Psychological Confrontation
- What were their objectives? How could they be modelled?

- Wanted to accommodate strengths of other approaches, cut out weaknesses

- Chose theoretical objective of

‘System Shock’

- Rooted in Soviet concept - ‘udar’
- Render enemy passive
- Render enemy action ineffective
- Attack entirety of enemy system
- Focus on operational level


WORLD
Strategy
Operations
Tactics

Basics – Elements

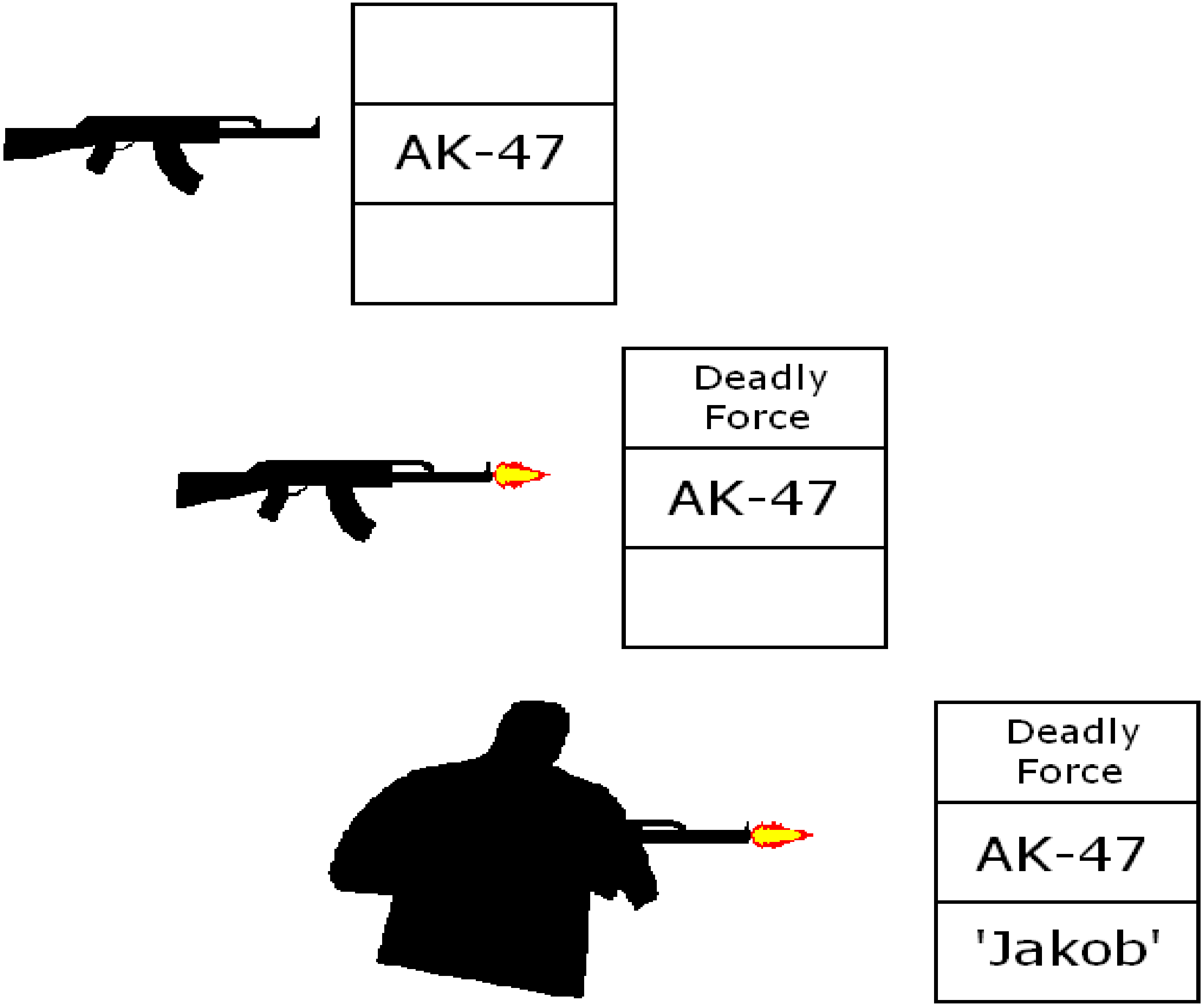
- We tend to see world in terms of elements
- Books, rifles, light bulbs, air, are all elements
- Events and operations can also be elements. A robbery is an element. An explosion is an element.
- Could define operations as collections of elements.

Basics – Properties

- Elements can be misleading.
- Operations better defined in terms of properties.
- Elements express properties.
- Mass, force, heat are properties
- Humour, fear, leadership are also properties

Basics - Conductors

- Elements do not express all their properties all the time.
- Something has to make the element express its property in the operation.
- This is the conductor.
- Conducting is a property in its own right.
- Usually refer to the conductor by name.



AK-47

Deadly Force

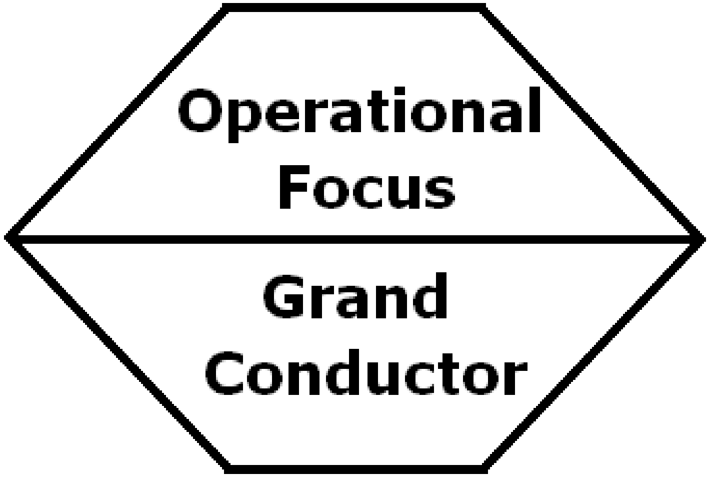
AK-47

Deadly Force

AK-47

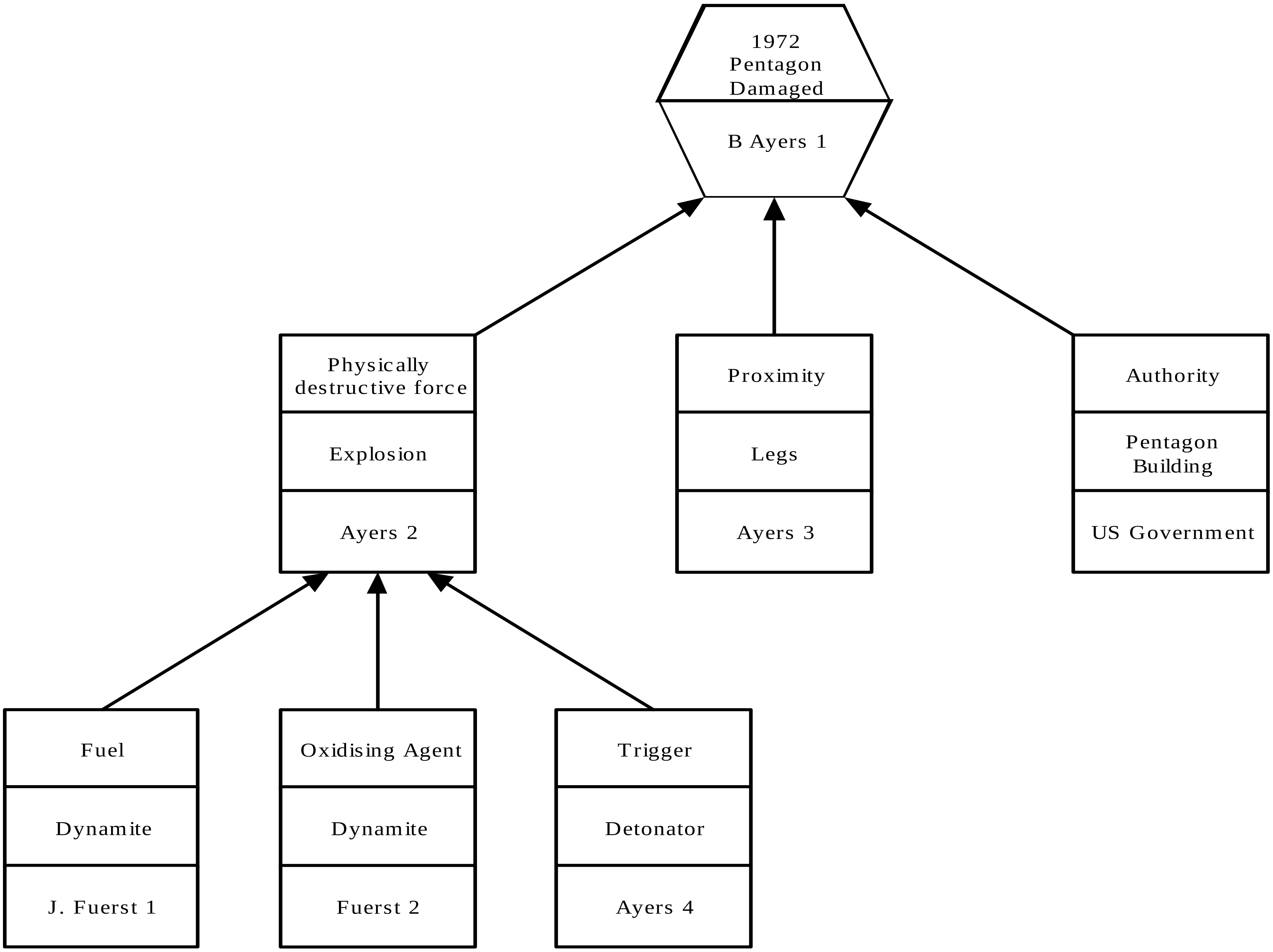
'Jakob'

Operations involve several groups of these property-element-conductor triads in concert.



Hence

“Operational Concert”

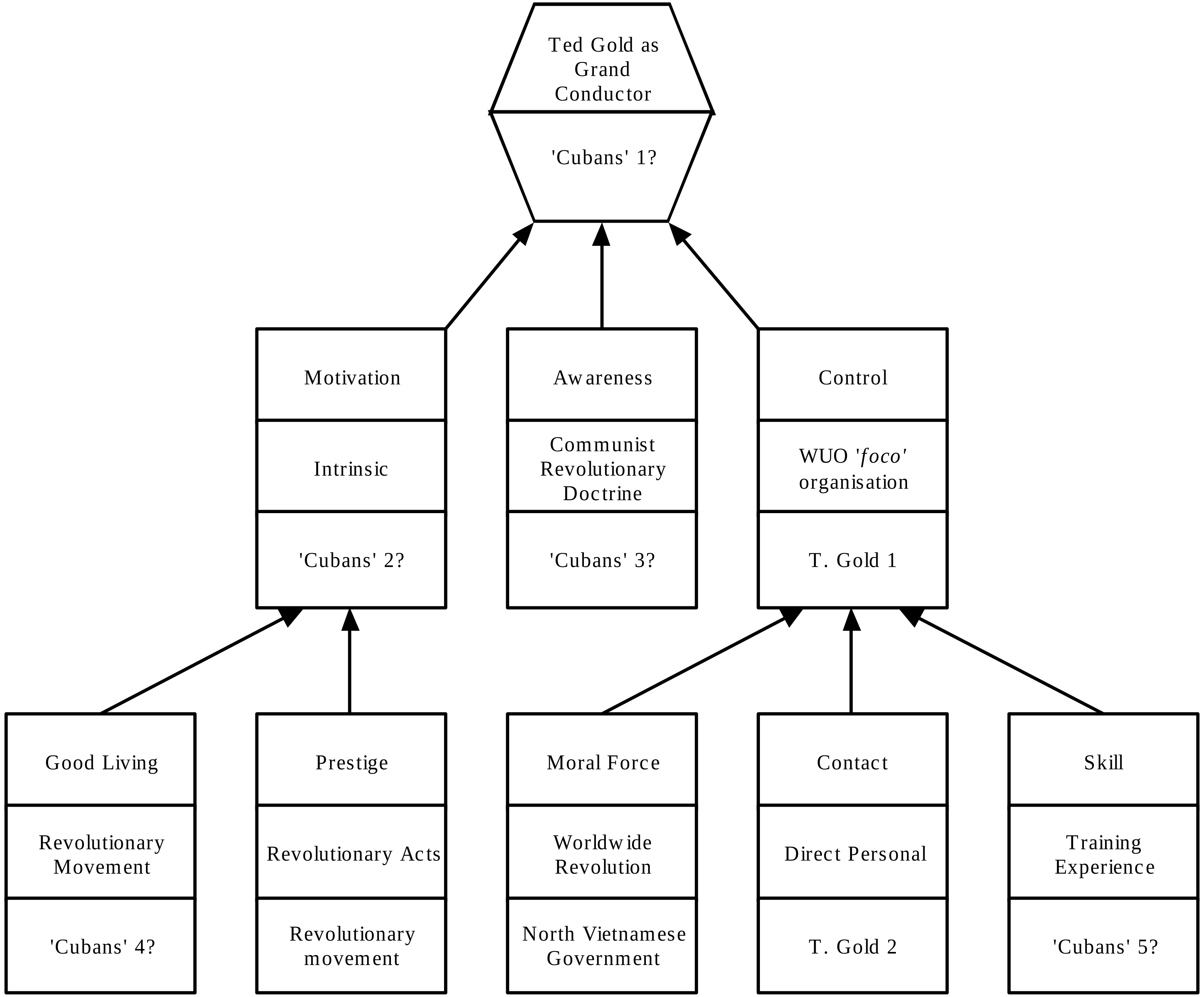

1972
Pentagon
Damaged
B Ayers 1
Physically
destructive force
Explosion
Ayers 2
Proximity
Legs
Ayers 3
Authority
Pentagon
Building
US Government
Fuel
Dynamite
J. Fuerst 1
Oxidising Agent
Dynamite
Fuerst 2
Trigger
Detonator
Ayers 4

Inflicting damage

- Several routes, depends on what you know
- Just properties:

- Sense, monitor, cap

- Elements –cripple expression of property. Ensure property is hit, not just element.
- Conductors – elaborate conductor concert. Send into system shock.
- Every time a gap is filled in, another target is presented.


Ted Gold as Grand Conductor
'Cubans' 1?
Motivation
Intrinsic
'Cubans' 2?
Awareness
Communist Revolutionary Doctrine
'Cubans' 3?
Control
WUO '*foco*' organisation
T. Gold 1
Good Living
Revolutionary Movement
'Cubans' 4?
Prestige
Revolutionary Acts
Revolutionary movement
Moral Force
Worldwide Revolution
North Vietnamese Government
Contact
Direct Personal
T. Gold 2
Skill
Training Experience
'Cubans' 5?

Damage Recovery 1

- Damage to an operational concert is rarely permanent.
- ‘Ideal’ process is:

Conductor of damaged property is alerted.

Conductor communicates to superior and or colleagues about problem.

System resolves problem.

Damage Recovery 2

- Resolving the problem can occur in three ways

  Element repair

  Element replacement

  Operational mutation/compensation
- Increasing difficulty for attacker.

Attacking damage recovery

- Can attack recovery operations
- Prevent realisation
    - Clandestine attack on elements
    - Clandestine severance of communications during regular attack.
- Provoke needless recovery
    - Shut down communication channels; conflicts with monitoring imperative
    - Manipulate impression of property; requires specialised effort; strategic deception
- Agitate and expose recovery critical persons.

Uses

- Knowledge sharing – test users liked
- Planning attacks on known networks
- Planning action against hypothetical operations – e.g. dirty bomb over London
- Threat assessments – take known operation, fill in elements and conductors.

Instructions Not Included

- Model intended to capture expert knowledge to guide attacks. User dependent. User centred.
- Tested in mock-ups, and with historical analysis, not live.
- Much more work needed.
- Principles as important as model

Principles

- Modelling can be used to assist counter-terrorism
- Any approach must be able to cope with partial information
- System shock is flexible but clear objective
- Damage and recovery are linked
- Seemingly distinct operations can share architecture.

Questions?