

**Threat and Risk Assessment :
A Soft Systems Type
Approach to Scenario Analysis
in Security Threat Analysis**

Threat and Risk Assessment

A Soft Systems Approach

“Between 1998 and 2001 the FBI and CIA received information from several sources that terrorist organisations, including al-Qaida, were planning some sort of attack with hijacked aircraft.

One plot that was identified involved flying an explosive-laden aircraft into the World Trade Centre. Neither the FBI nor the Federal Aviation Authority Administration acted on the Information, however, because they ‘found the plot highly unlikely’. It was, but it was possible”

The London and Manchester Guardian. November 8th 2005

THE SYSTEMS APPROACH

Is a way of looking at some part of the world, by choosing to regard it as a system, using a framework of perspectives to understand its complexity and undertake some change process.

THE SYSTEMS APPROACH

KEY CONCEPTS

HOLISM - looking at things as a whole and not as isolated components - connectivity

SYSTEMIC - Pertaining to a system, treating things as systems, using systems ideas, adopting a systems perspective.

APPLYING RISK MANAGEMENT CONCEPTS TO SECURITY

In security risk management, risk is usually calculated as -:

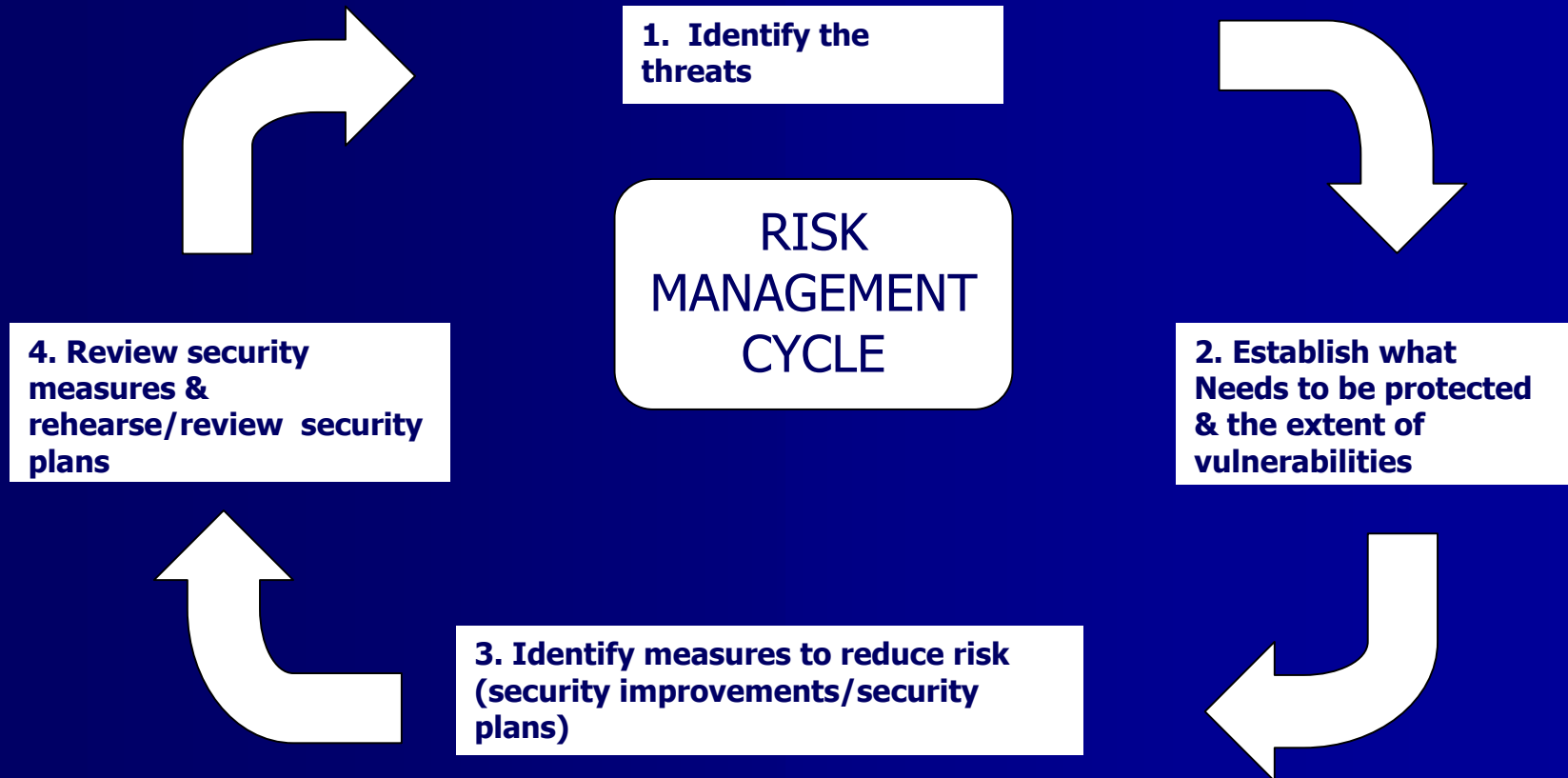
$$\text{Risk} = [\text{Threat (T)} \times \text{Vulnerability (V)}] \times \text{Consequence (C)}$$

Threat is a measure of the likelihood that a specific type of attack will be initiated against a specific target (i.e., a scenario)

Vulnerability is a measure of the likelihood that various safeguards against a scenario will fail.

Consequence is the magnitude of the negative effects if the attack is successful. Some organizations, including the US Navy, use the term criticality to describe the impact of an event.

Risk Management Cycle



Terrorist Threat Assessment

A Credible Threat?

- **Is the location / event an inherently attractive target? A Government Building may a more attractive target than an shared occupancy office block**

However, in terms of vulnerability, the level of security at the former may encourage an attack at the latter

Risk Impact and Probability

PURPOSE

To evaluate the risk to the asset
To quantify risk and establish which risks are acceptable and which are not.
To determine what measures and costs are required to reduce unacceptable risks to an acceptable level

Identify Assets and mission

Determine Credible Risks

DETERMINE
RISK LEVEL
FOR EACH THREAT

		Vulnerability to Risk			
Impact of Loss		Very High	High	Moderate	Low
Devastating					
Severe					
Noticeable					
Minor					

Risk Rating Interpretation

DETERMINE
ACCEPTABILITY
OF RISK

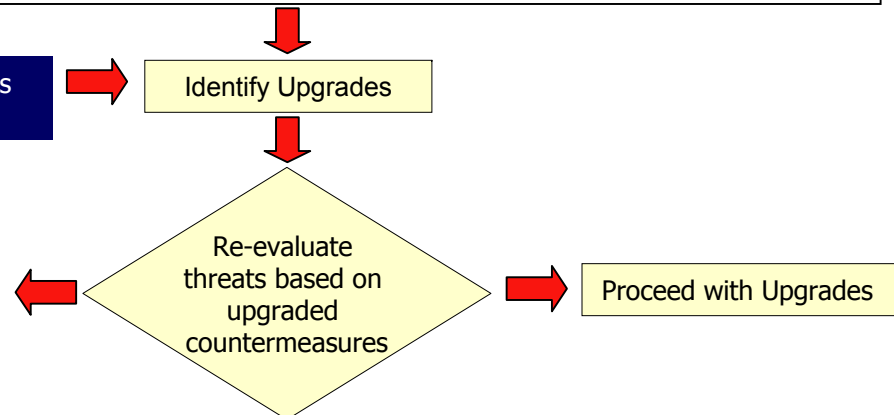
	These risks are very high. Countermeasures recommended to mitigate these risks should be implemented as soon as possible.
	These risks are moderate. Countermeasure implementation should be planned in the near future.
	These risks are low. Countermeasure implementation will enhance security, but is of less urgency than the above risks.

Repeat if Risk Ratings
are not Reduced

Identify Upgrades

Re-evaluate
threats based on
upgraded
countermeasures

Proceed with Upgrades



Soft Systems Analysis

Rich Pictures

Rich Pictures

A representation of the problem domain unstructured. A diagrammatic representation of the problem domain which seeks to encapsulate and represent "soft" and "hard" data and information

The Meeting of European Leaders at Hampton Court Palace October 27th 2005

QuickTime?and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

The Meeting of European Leaders at Hampton Court Palace October 27th 2005

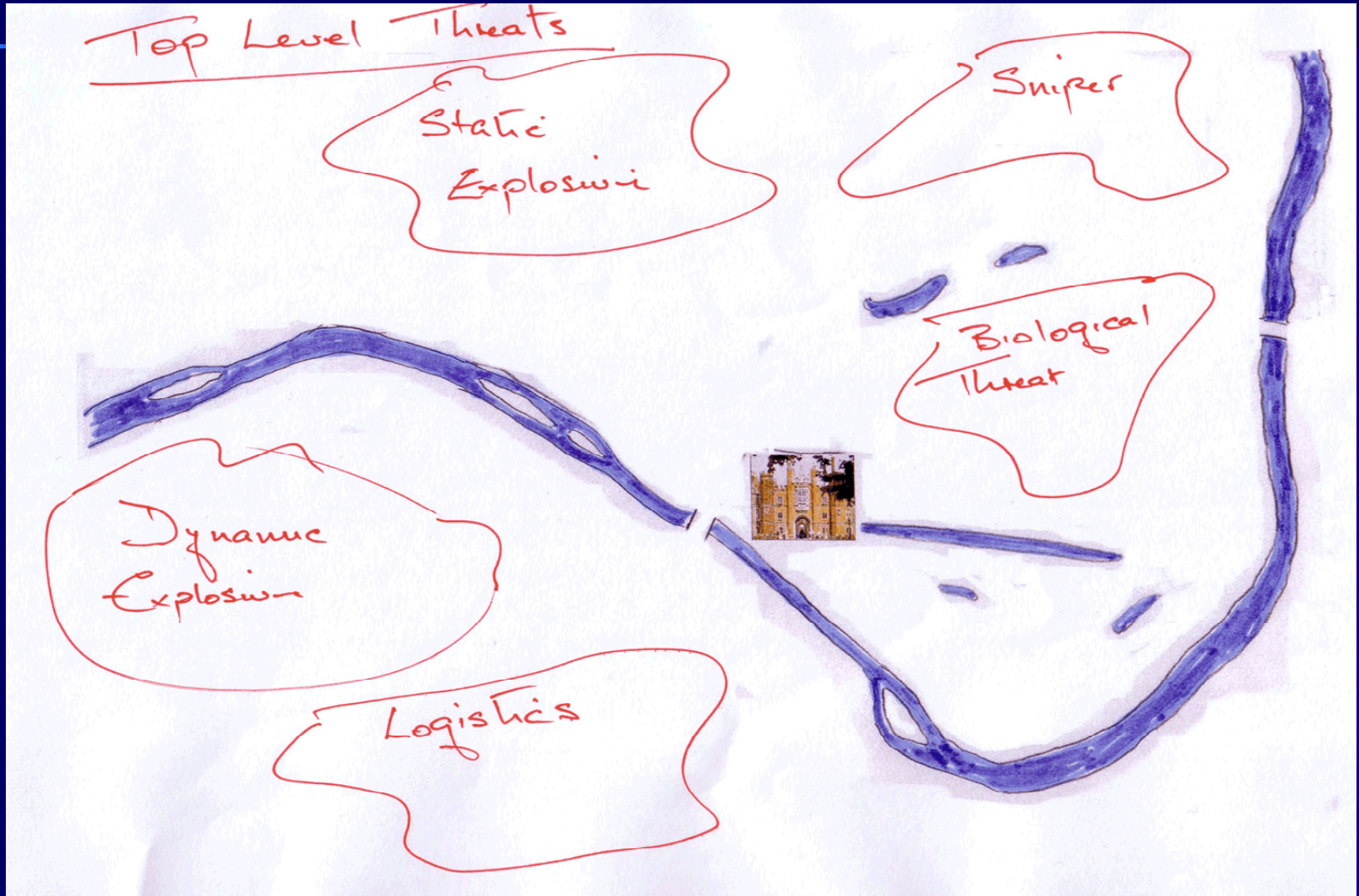
QuickTime and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

The Meeting of European Leaders at Hampton Court Palace October 27th

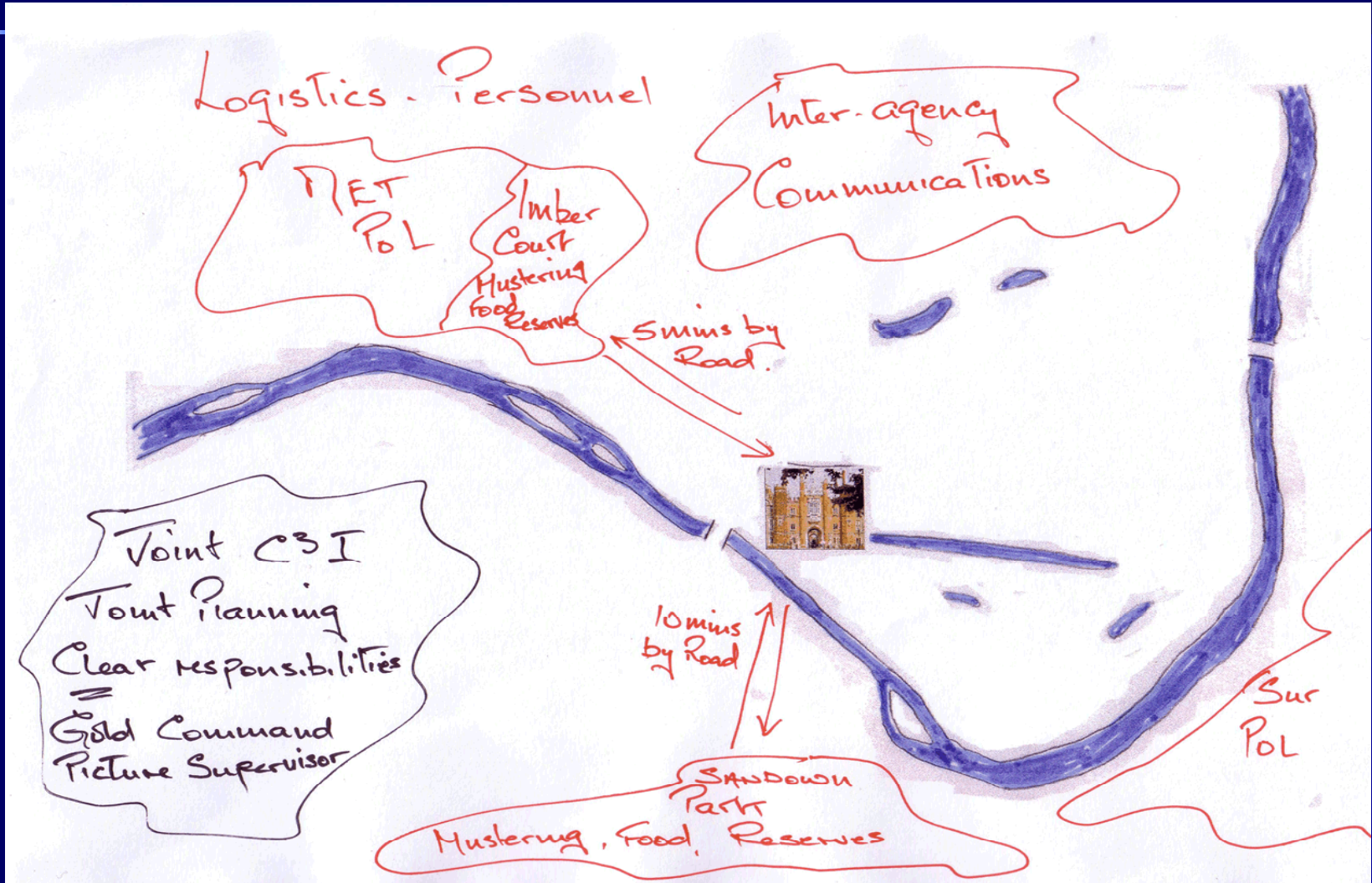
2005

QuickTime?and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

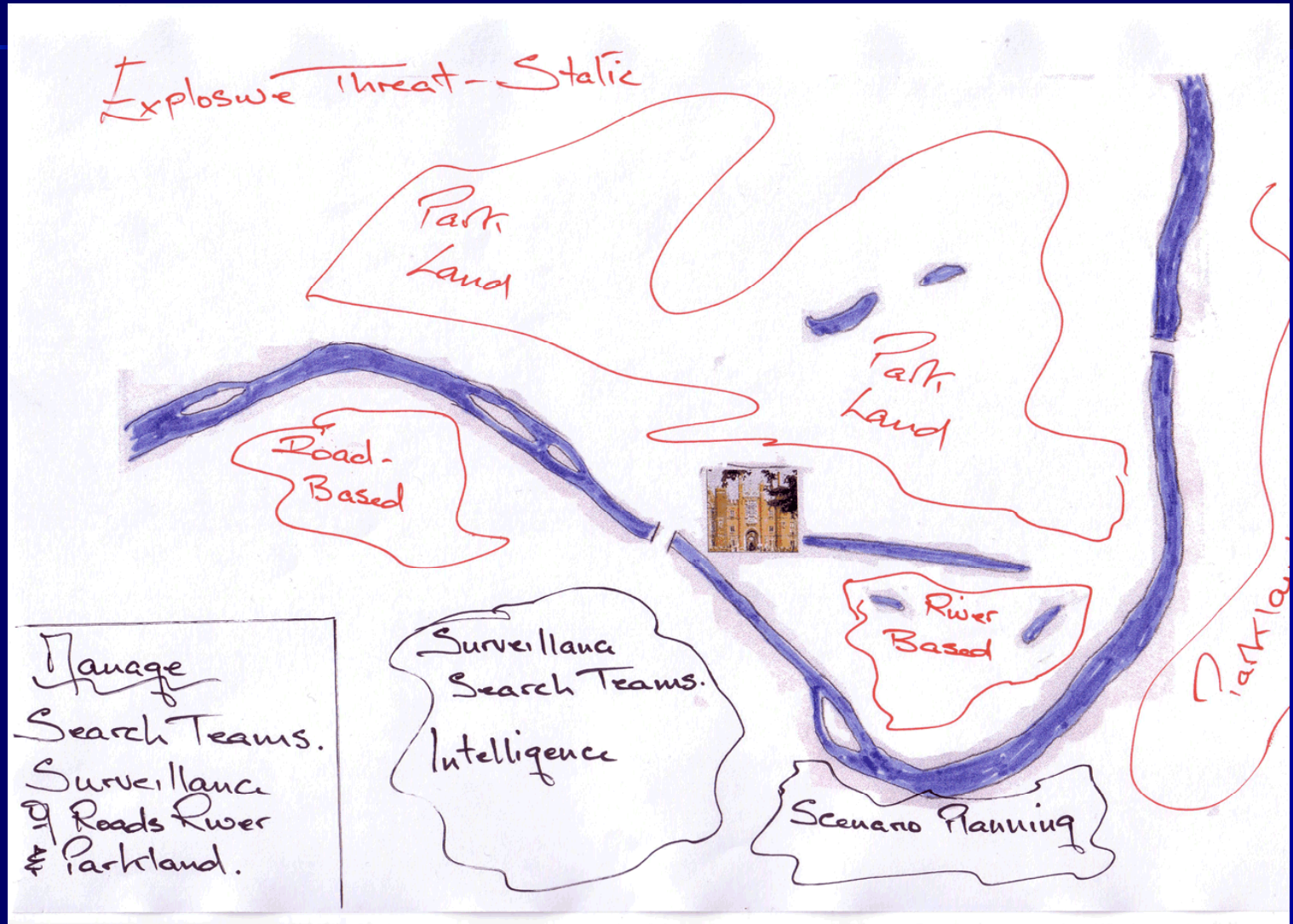
The Meeting of European Leaders at Hampton Court Palace October 27th 2005 (Top Level Threat)



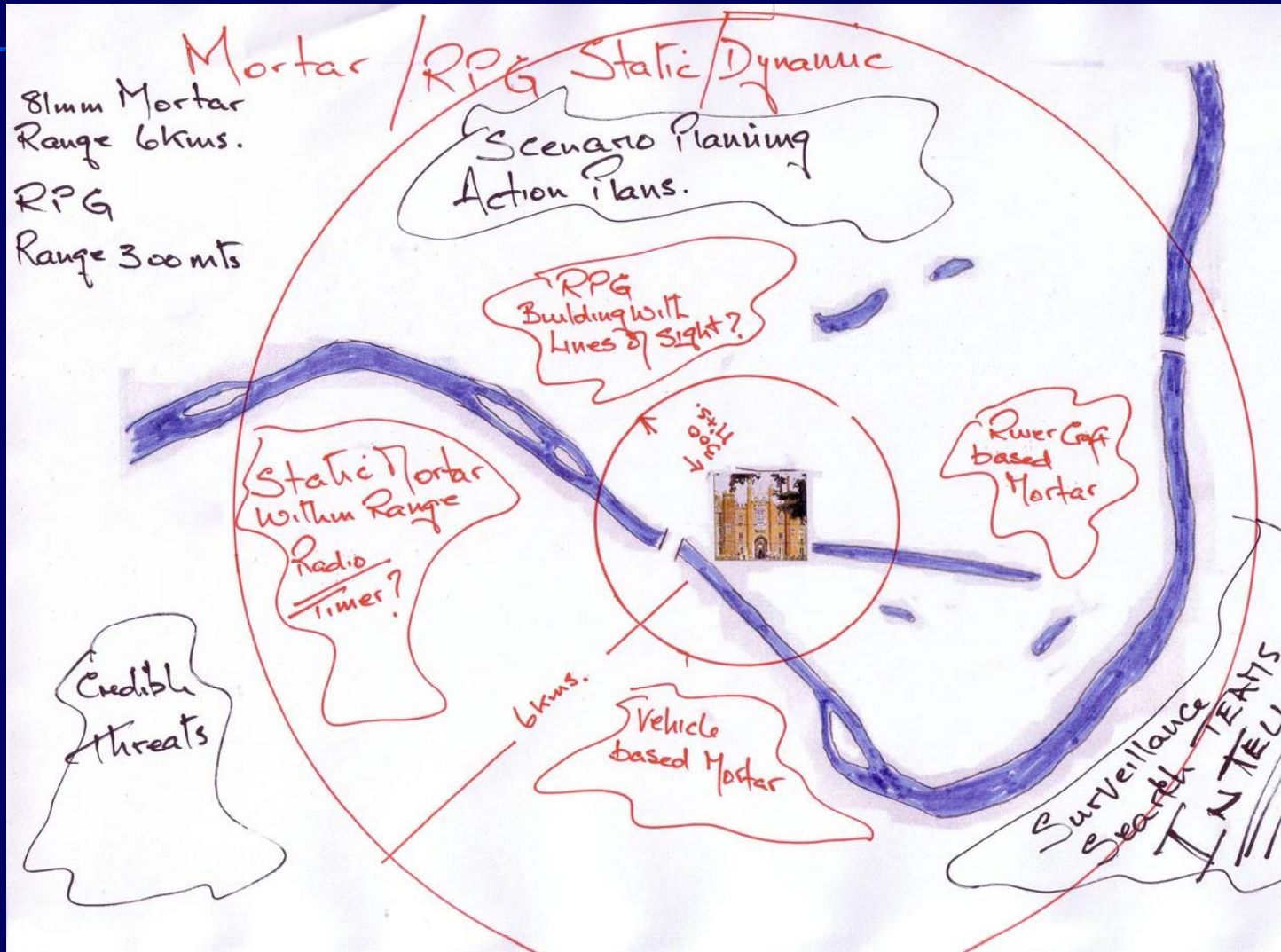
The Meeting of European Leaders at Hampton Court Palace October 27th 2005 (Logistics)



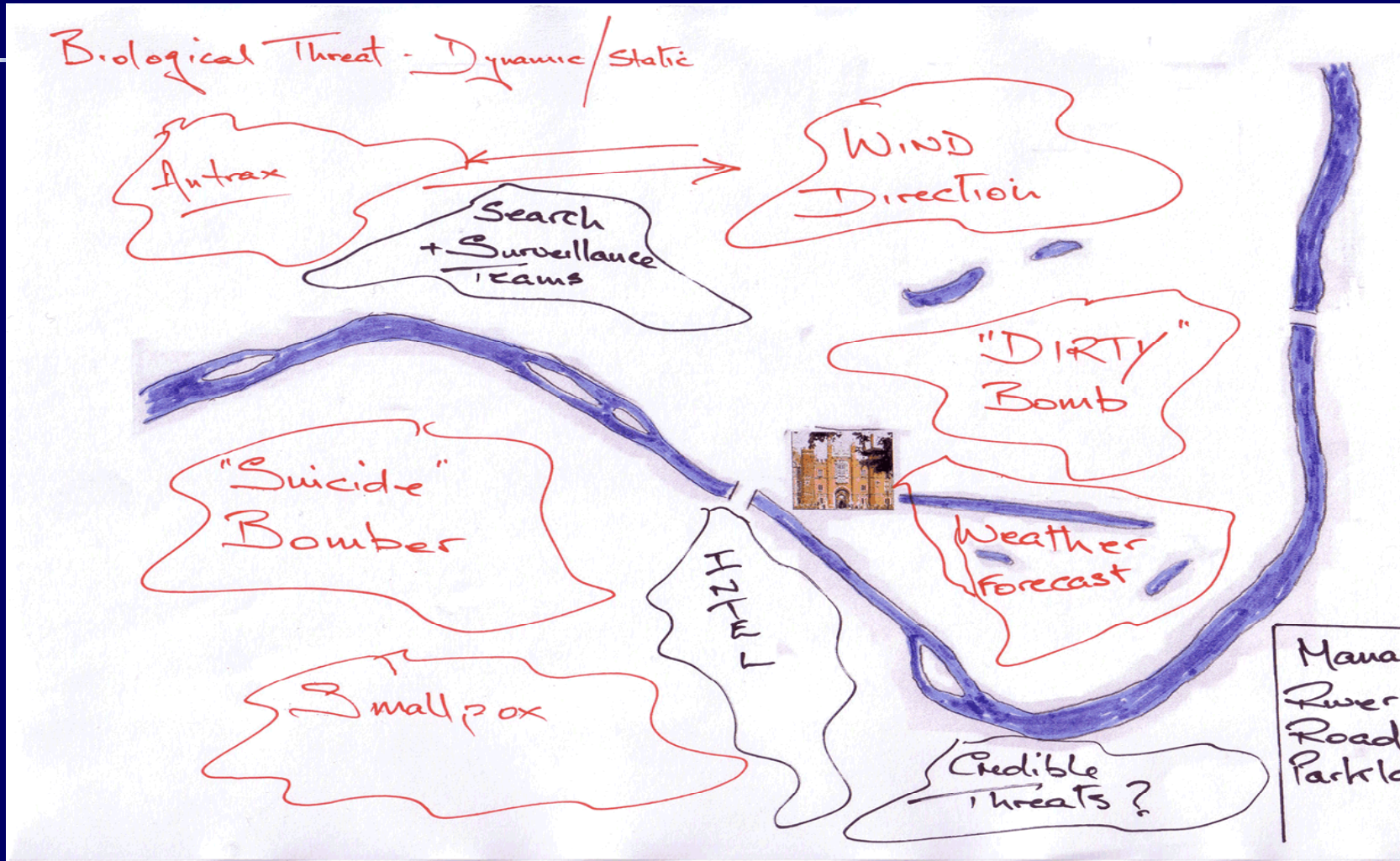
The Meeting of European Leaders at Hampton Court Palace October 27th 2005 (Explosive Threat)



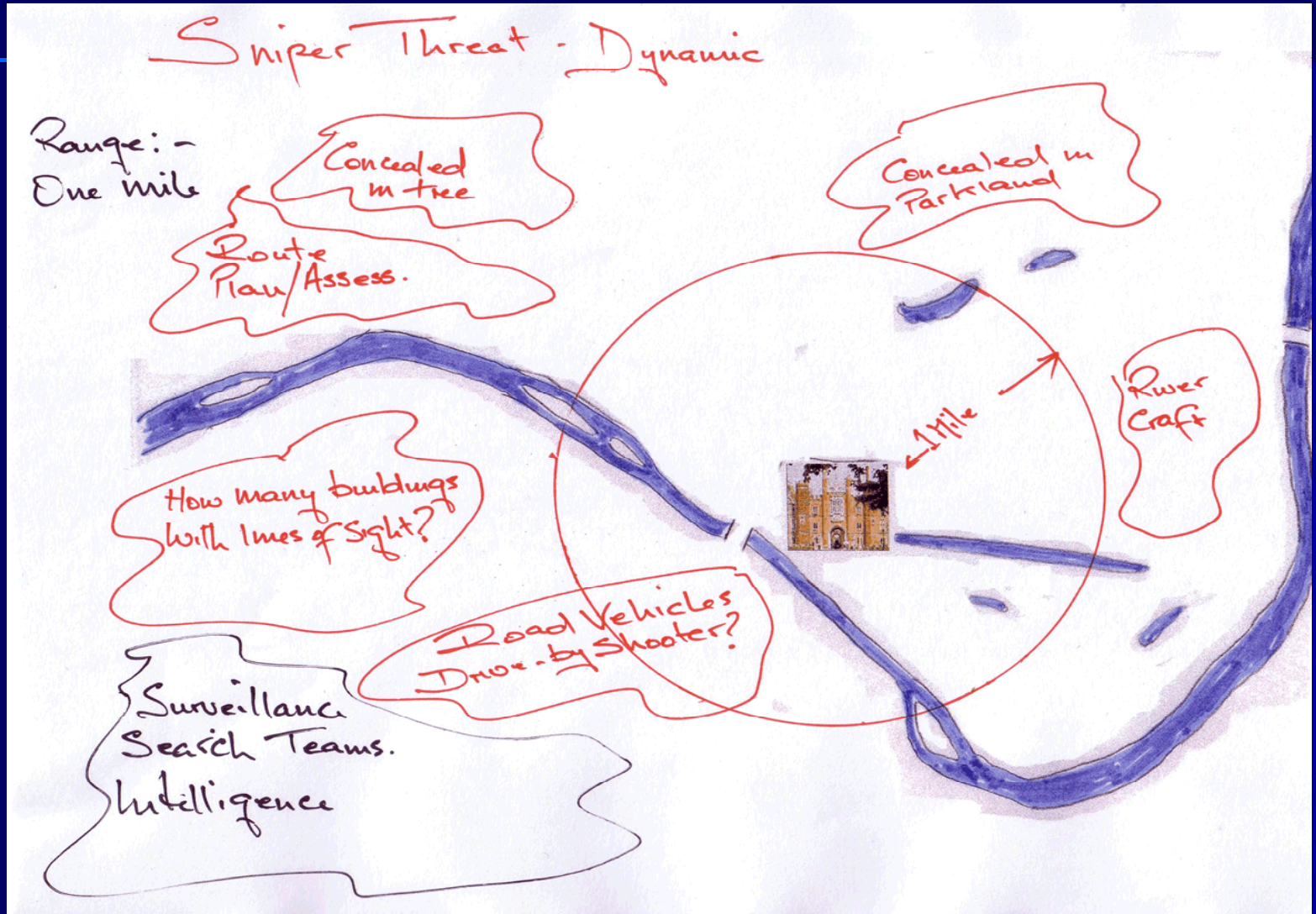
The Meeting of European Leaders at Hampton Court Palace October 27th 2005 (Mortar Threat)



The Meeting of European Leaders at Hampton Court Palace October 27th 2005 (Biological Threat)



The Meeting of European Leaders at Hampton Court Palace October 27th 2005 (Sniper Threat)

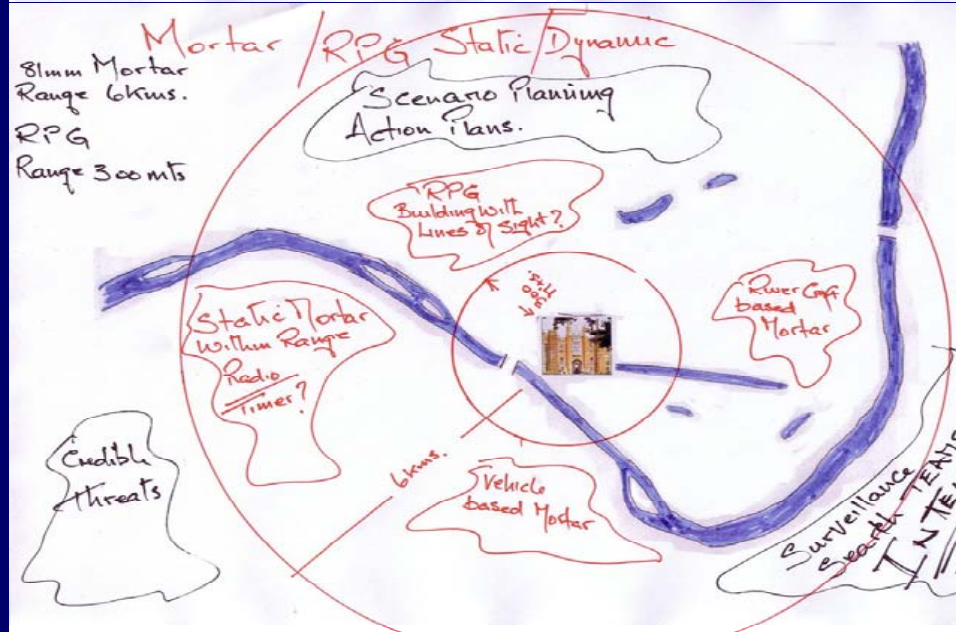
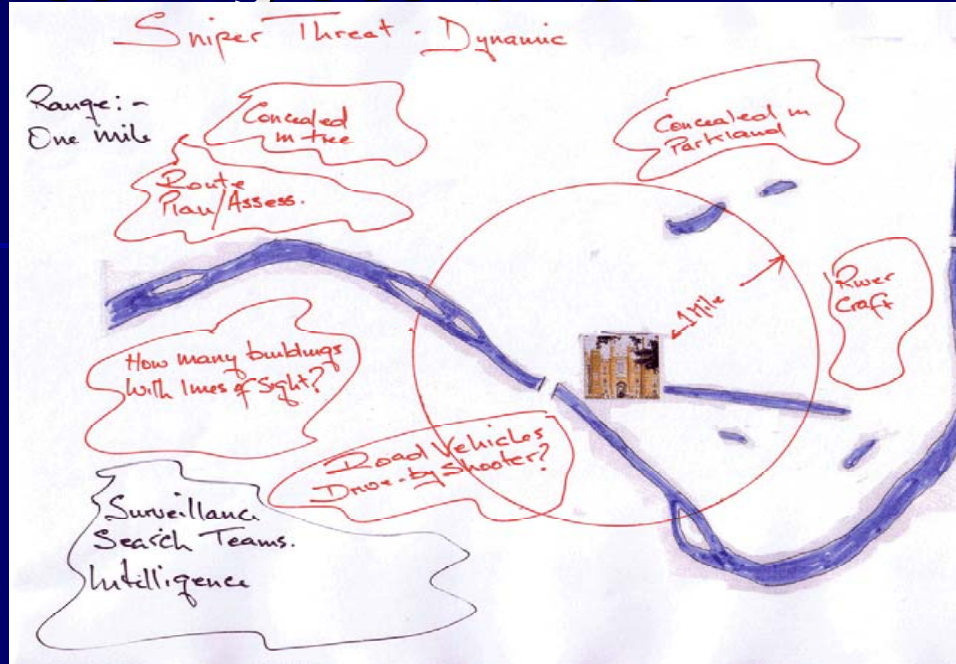


Rich Pictures

Cross-checking Scenarios

Once each scenario has been explored in sufficient depth of detail using second and subsequent levels of Rich Pictures, it is possible to check each aspect of each scenario backwards, through the interlinking picture-based chain of analysis.

Cross-checking Scenarios



Cross-checking Scenarios

<i>Rich Picture</i>	<i>Scenario</i>	<i>Comments</i>	<i>Applicable to other Scenarios?</i>	<i>Included in Scenario?</i>
Ó Sniper Threat Dynamic Ó	Route : Plan & Assess	Inspect and assess all probable line of sight vantage points giving ground level view through glass of VIP vehicles	Yes	Yes
Ó Mortar/RPG Static /Dynamic Ó	Route : Plan & Assess	-O- Initiate Remedial Action	Yes	No
Ó Explosive Risk Static Ó	Route : Plan & Assess	-O- Initiate Remedial Action	Yes	No
Ó Logistics Personnel Ó	Route : Plan & Assess	N/A	N/A	N/A