

Expand, Collapse and Auto-Redraw the Threats Hierarchy

Expand All will expand all branches of the hierarchy.

Collapse All will collapse the hierarchy and show only the goal and the first level of elements (threats).

You can also expand/collapse **sections** of the hierarchy by clicking the same icons at the left of the threat node.

When the **Auto-Redraw** box is checked, clicking on the *name* of any element will not only expand the branches below that element but will automatically contract the branches in other parts of the hierarchy. This is useful to be able to focus on a part of the hierarchy, see all of its ancestries, but not be distracted from details in other parts of the hierarchy.

The screenshot displays a user interface for managing a threat hierarchy. At the top, there is a control bar with the following elements from left to right: a dropdown menu set to 'Tree View', an 'Expand All' button, a 'Collapse All' button, an unchecked 'Auto-Redraw' checkbox, a blue 'Add' button with a plus icon, and an 'Edit' button with a pencil icon. Below the control bar is a tree view of threats. The root node is 'Threats', which is expanded. It contains five main categories, each with a square icon and an information icon (i): 'Human Factor', 'Environmental', 'Infrastructure', 'Terrorism', and 'Technology'. Each category is further expanded to show its sub-threats. A mouse cursor is visible over the 'Environmental' category node.

- Threats
 - Human Factor
 - Inadequately Trained Staff
 - Disregarding or Not Following Proper Policies, Processes, or Procedures
 - Lack of Situational Awareness
 - Engineers Failure to Properly Install Equipment
 - Environmental
 - Flooding of Intelligent Event Monitoring Infrastructure
 - Lightning Striking Signaling Infrastructure
 - Infrastructure
 - Minor Electrical Power Shortage
 - Major Electrical Power Loss
 - Mechanical Failure of Sensors
 - Mechanical Failure of Signals
 - Mechanical Failure of Cables
 - Terrorism
 - Conventional Attack on the Signalling Infrastructure
 - Cyber Attack on the Intelligent Event Monitoring Network Itself
 - Cyber Attach on the Telephony and Broadband Infrastructure of the Service Provider
 - Technology
 - System Software Technology Obsolescence
 - System Hardware Technology Obsolescence
 - New Cutting Edge Software Technology Available
 - Intelligent Monitoring System Software Failure