



## Network Disruption Harmonics: A new model for cross domain warfare and analysis by White Wolf Security

### **Introduction**

All students and practitioners of information operations are familiar with the science of networks and the notion of cascading attacks. The science of networks is about studying the relationship of nodes, hubs and the links that connect them. Specifically, much has been written about scale free networks and their relative strength and weaknesses. Cascading is another topic familiar to those in this arena. The concept of cascading is simple, an attack or incident against one infrastructure will have a cascading effect against others. All of this is well traveled content and useful to planners. However, cascading is a linear progression that fails to adequately represent the non linear nature of networks. Cascading also does not address the issues of dampening and amplification.

To address the limitations of cascading we have created a new model for forensic and predictive modeling of attacks against a network. This new model replaces cascading with harmonics. Harmonics and wave propagation more adequately represent the true interactions between nodes on a hub. Under cascading theory, nodes must be connected in order to interact. Using a harmonic theory, nodes can be affected in several ways regardless of their connectedness.

This paper is designed to deliver a new model for mission planners, infrastructure defenders and forensic responders. The model of network disruption harmonics is better adapted to address cause and effect across multiple domains of a scale free network.

### **Network Disruption Harmonics**

Everyone is familiar with general wave theory. Throw a rock into a pond and concentric rings of waves propagate out from the point of impact. The same is true to activity within a scale free network. An incident within a node will send out concentric rings of wave. These waves represent first, second and third order effects. Generally, the farther out from the incident a wave is, the less its impact, but the greater its audience. If another node on the network is within reach of these waves, they will be affected accordingly and set off their own set of waves. For nodes that are too far away to be directly affected by the first, second and third order effects, there is another transmission media; the link itself. Strong links will transmit a greater amount of wave energy between nodes than weak links. Again, when the wave energy hits another node through its link, it will again set off its own set of waves. This model more adequately represents the true interactions between nodes during incident activity.

### **Different Types of Nodes**

Another failure of the cascading model is its inflexible view of the world. Not all nodes in a network are the same. The NDH model allows for two primary types of nodes; amplifiers and dampeners. Amplifiers are those nodes that amplify the incident wave activity. By intent or accident, an amplifier node will add intensity to an incident on a network. An example of this is a power failure at a 911 call center. The incident by itself becomes a minor nuisance as the call switches re-route call traffic to a secondary



site. However, if the power outage occurs at the same time as a mass casualty causing event, the downed node now is an amplifier causing significant delays and confusion.

On the opposite side are dampening nodes. These are nodes that are adept at absorbing wave energy and slowing down or stopping wave propagation all together. An example of a dampening node could be a simple riot control line; group of police who absorb the energy of a mob and prevent it from propagating past a specific point.

Nodes are also multi-dimensional. There are any number of dimensions that you can carve a network into. For example, when using NDH for mission planning, you can divide the node space into physical and cyber. Some nodes will be primarily one dimensional. A ship at sea is an example of this (albeit there is a nominal cyber component that represents communications). An email server is primarily a one dimensional cyber node, while a SCADA server controlling electricity is equal parts cyber and land. Links can also carry nodes between dimensions. A primarily physical asset can be carried over to cyber through unsecured network connections. Finally there are also bridge nodes. A bridge node is any node connecting two or more dimensions. Examples of bridge nodes include ports (land and sea), airports, wireless access points and cell phones.



## Diagramming the model

Figure 1 is a sample network disruption harmonic diagram. The cyber and physical arrows indicate that this is a two domain diagram. Where the arrows converge, so too do the cyber and physical domains. At the opposite end of the spectrum are those assets that are not converged. In this diagram, the **red** represents the primary event on the networks. The three lines of varying thickness around the node represent first, second and third order effects. The lines linking the nodes represent networked links. Thicker lines represent stronger connections. The red node experiences its first, second, and third order effects. The blue and green nodes are too far removed from the incident epicenter to experiences those ripples directly; however, because of their connections they receive shocks via the network and then resonate their own first, second, and third order effects outside of the primary node. The effect of the incident travels through the link and sets the blue node vibrating with its own incident.

The **yellow** node feels the impact of the third order effect from the primary event as well as through its own link. As such, it too begins vibrating in response to the incident and so on and so forth. Of particular note is the small unlinked black node. It too will feel the effect of the various incidents. In most cases the unlinked node represents psychological or economical responses within a single domain.

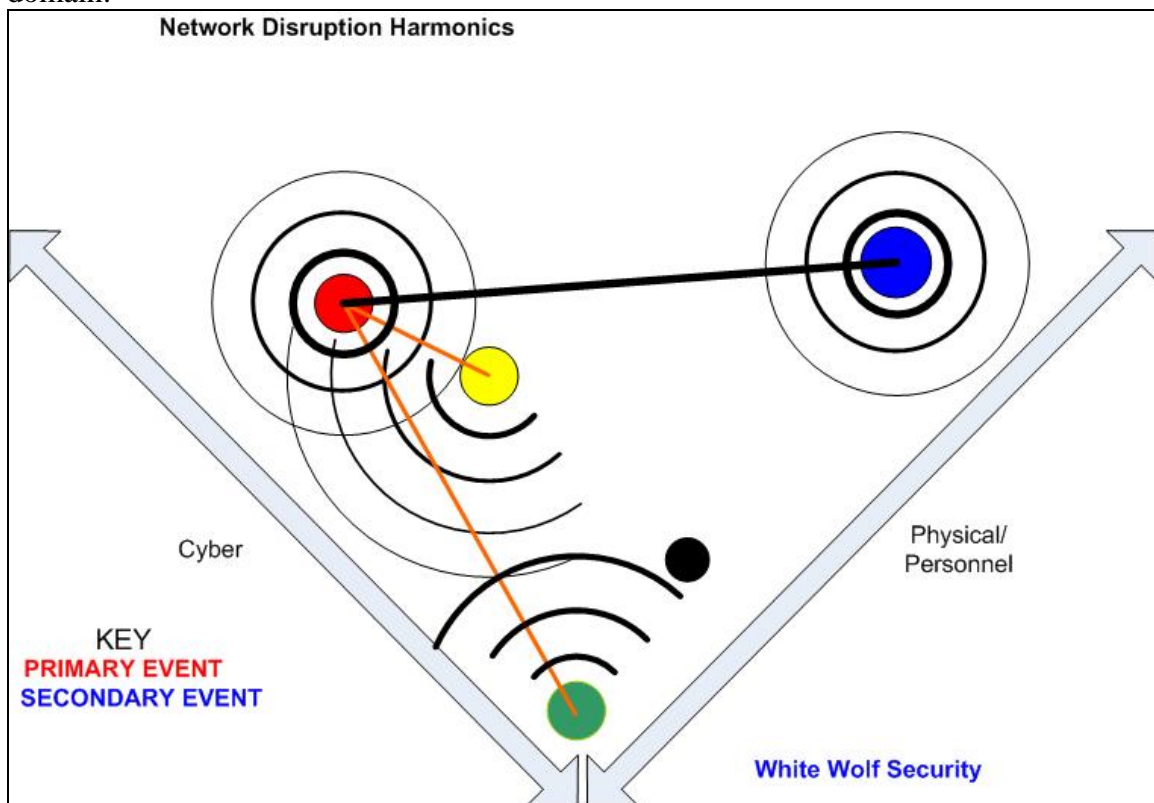


Figure 1 - SAMPLE NETWORK HARMONIC DIAGRAM

## Conclusion

This short paper is designed to provide an alternative network disruption model; one that accurately represents how nodes on a network respond to an incident. Future



updates to this paper will include examples of practical application of the model against real and planned events.

If you would like more information or a presentation of this or any of our papers, please contact Joe DeCree at 717-898-9654.

### **White Wolf Security**

White Wolf Security is a provider of high-end, tailored, hands-on Information Security training. We are unique because our courses move beyond the technology. Our diverse team of instructors is pulled from a variety of backgrounds. As a result, we are able to address the Technical, Legal, Policy and National Security issues that surround information and its uses.