**Discussion of Practitioner Questions**

**What warning indicators would you expect leading up to the scenario?**

* Some sort of reconnaissance
* Unknown behavior coming across intrusion detection system
* Some geopolitical event is going on to drive the attack
* They are finding minus day warnings in some of the attacks
* Hackers are doing pilot deployments of the attacks
* Routine daily reconnaissance, political lead up, and/or scaling up of operations.
* Define what question what you want to answer and knowing it in advance you understand what you are looking for.
* Commercial networks are going to see indicators first
* Indicators in the supply chain
* How to protect the people then identify what threats are out there to affect them.
* Three different levels of indicators are the technical indicators, external indicators, and internal indicators.
* The context of the situation would lead to the indicators
* Apply multiple contexts to a scenario to generate multiple hypotheses
* Customers can be a good indicator (Hey I clicked on bad link or computer is not working)
* What are reasons people want to attack me? What resources do I have that people want? Who wants those resources or assets?
* Base indicators are important (What is normal) then determine what is not normal.
* Indicators that you care about need to map out of the actions that you would take
* Validity and credibility of data

**What are the sources of that type of information?**

* Rearview mirror context (ingredients of a prior event)
* Knowing the results of your own testing (internal)
* Pinging the system in various different ways
* Flocking and herding philosophies from nature and apply it to web network traffic.
* Modeling the network traffic in terms of types of traffic, domain, or volumes of traffic.

**Other comments**

* What do we actually want to remediate (time, money ROI)?
* Being consumers of the finished analysis and making a decision
* How much resources do we devote to how serious the situation
* Have meta data about data that relates it to people (ability to put a confidence number to it)
* There needs to be someway to categorize the threats and how serious they are.
* Distinction between government and industry is going away fast
* What is a way for the offensive side to help the defensive side
* Information market to leverage judgments without giving up information
	+ Attack tools
	+ Making use of the offense
* Connecting info and context to give it significance
* Predictive analysis futures market
* Changing the relationship between the private and public sector
* How can you build trust that does not necessarily involve the classic government trust with clearances etc.
* Sharing protected data vs. sharing judgments and context
* Consortium of judgments from governments and industries
* Sharing attack information among companies without stating financial losses

**What sources that you would like to have**

* Open sources
* Delay in publication by CIRT
* Foreign language sites are under exploited because they use their language as defense
* Need Savvy linguists
* Look more into dark webs because they are not online but available
* Using watchdog groups like the one in Russia to help see different attack locations
* Policy issues that prevent using the info that companies have because of legal concerns
* Infinite number of databases (Social networking, facebook)

**Tools**

* Too many tools
* Tool that connects you to a person that can help you is better than a tool that links you to another piece of data
* A-Space at DNI
* Wikis like Intellipedia
* Feature vector of an attack to connect you to a reputable source with prior experience