Topic 3: Technologies to support International data exchange.

How would it build beyond /integrate with the PREDICT framework

- Develop common view on what should be measured and how (measurement methodolody)
- Consider creating public (anonymized) datasets
- Establish a series of events (i.e. conferences, workshops) where publishing raw data would be prerequisite

Indicate incentives for data providers, eg Russian entities to contribute

- Cooperation in shutting down botnets with overseas C&C
- Solid scientific results with better experimental data coverage
- Increase transparency

How would it address proliferation of malware

- Public datasets to stimulate research activity
- Faster and less faulty detection algorithms
- Quicker incident response

What type of data are needed for an empirically-grounded science of security and what system does each data class help with.

- Malware body, shellcodes (honeypots, IDSs)
- C&C communication statistics (netflow exports)
- First-stage analysis results, i.e. malware behavior statistics at host and network levels, numeric datasets (experimental research frameworks)

Author(s) name and institution