Optimizing Lawful Responses to Cyber Intrusions

Dr. Bret Michael, Naval Postgraduate School
bmichael@nps.edu

Tom Wingfield, Esq., Potomac Institute for Policy Studies
twingfield@potomacinstitute.org

Dr. Duminda Wijesekera, George Mason University
dwijesek@gmu.edu

Disclaimer

- The views and conclusions contained in this presentation are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.

Acknowledgements

- Naval Postgraduate School's Homeland Security Leadership Development Program
- George Mason University Critical Information Infrastructure Program

Problem Definition

- Cyber intrusions have three legally problematic aspects
  - High-speed
  - New techniques
  - Unidentified actors

High Speed

- Requirement to provide legal advice to decision-makers in near-realtime
- Many inputs may be automated for rapid collection, analysis, and response
- Human judgment still required, so process must be made as efficient as possible

New Techniques

- Limited legislation and case law
- Limited reserves of experts with deep operational law experience
- Paradoxically, new situations require return to first principles
- Example: for military operations, *jus ad bellum* and *jus in bello*

Unidentified Actors

- Normally, legal analysis *starts* with identity of actor; usually not possible during cyber attack
- Characteristics of *actions* and *target* is key
- Three legal regimes
  - Law Enforcement
  - Intelligence Collection
  - Military Operations

Key Attributes

- Parallel trees with binary decision structure
- Resources *collected*, *organized*, *prioritized*, and *abstracted* for each decision point
- Means for providing *audit trail* and *brief builder*
- Collaboration, retention, simulation, and comparison
- Open Source development

Conclusion & Summary

- An academically comprehensive and operationally useful **legal framework** is needed to address the growing threat of cyber intrusions
  - Serve as the basis for the **seamless application** of the law to criminal, military, and espionage activities in cyberspace
  - Built and maintained using an **open source architecture**
    - Review of the law governing these intrusions, and its distillation into two interconnected decision trees

Comparison of computer and human decision trees

Attribute	Computer tree	Human tree
Speed of decision making	High	Low
Need for human reflection and creativity	Low	High
Reliance on clearly discernable, objectively verifiable criteria	High	Low

Sources of information