Ontology of Cyber Crime: A Necessary Joint Effort

Shahriar Pourazin
Board Chairman, Sepehr S. T. Co. Ltd.
9th ETSI Security Workshop
15 - 16 January 2014
Sophia Antipolis, France
Overall Idea in Brief

- (Cyber) Crime Ontology is **already under Focus**
- Parts of (Cyber) Crime Ontology are **Reusable**
- Some reusable parts **may be Standardized**
- Some Standard parts are **NECESSARY**
- The Standard part **SHOULD BE**
  - Created as Standard Compliant
  - In Public Domain
  - Defined as a **Managed Open Project**
  - Managed by a **Standards Authority** (ETSI is suggested)
  - Supported by **Companies and Academic Institutions**
Other Efforts and Related Work

- A Domain Ontology: Italian Crime Ontology, Carmelo Asaro et al.
- An event ontology construction approach to web crime mining, Li Cunhua et al.
- A Domain Ontology to Support Evidence-Based Practice and Context Usage on Crime Prevention, Expedito Carlos Lopes et al.
- Cyber Forensics Ontology for Cyber Criminal Investigation, Heum Park et al.
- Ontological Crimes Against Humanity, Paul C. Santilli
- Building an Ontology that Helps Identify Criminal Law Articles that Apply to a Cybercrime Case, El Hassan Bezzazi
- Solving Crimes using Referent Tracking: Building a Realism-based Crime Ontology, Werner CEUSTERS
- Ontologies for Legal Information Serving and Knowledge Management, Joost Breuker et al.
- Cyber Forensics Ontology for Cyber Criminal Investigation, Arthur Mapanga
Reusable Parts of (Cyber) Crime Ontology

Reusable Parts: “They have done this already” so we can use it. “Forged Financial Transaction” has another instance. Please add it there. And this way we will have faster progress. We will give feedback. Their ontology will become more robust. Some examples:

- Unauthorized Use of Other’s Resources
  - Running Bots on Unaware Users’ Computers
  - Using Other’s Computer to Store Information
- Forged Financial Transaction
  - Making Forged Payment Statement
  - Changing the owner of the payment transaction
Standard Parts of (Cyber) Crime Ontology

Parts that SHOULD BE Standardized (Subset of or ideally the same reusable parts) We need to know the exact concept reference ID within their (cyber) crime ontology to communicate about the violations. We call it “Unauthorized Access” they call it “Access Rights Violation” But we are both talking about one thing.

- Illegal Access to Information
  - Hacking Sites for Stealing the Data
  - Fetching Files from Other’s Private Storage
- Forged Information Generation
  - Hacking Sites to Deface or Inject False Information
  - Sending False Messages
Why it SHOULD be Standard

- Larger Investment on Software and Service Projects
  - Location Independent Violation Reporting to Cyber Police
  - No Need for Re-Engineering the Forensics Subsystems
  - Effective Cross System Communication with SOC’s, CSIRT’s
  - Better Security Mastering According to Global View on Violations
  - Easier internationalization by Lower Cost Still High Quality Porting of Secure Software
  - Detecting the Conflicts between Legal Issues of Service Endpoints
  - Selecting the BEST Server Installation Site (Owner, Site, Labor, Client puzzle)

- Coordinating the Different in Detail Forensics Data
  - More detailed logging in locations that the activity is a severe crime
  - Different logging based on the local law about a criminal activity and privacy
  - A methodology toward Global Compromise between LI versus privacy

- Flexible Warning or Disclaimer Messages for Globally Visible Services
  - Displaying the CORRECT disclaimer statement based on the endpoints’ legal regulation
  - Warning about the support of a transaction according to other endpoints local law

- Per Path Security Policies based on the Request Source and Server Site
  - Partial access for service that will not comply local law of the other endpoint
  - Adding more levels of authentication for those clients from special locations

- Approval from Global Organizations and Affecting the Local Regulations
  - Digital Economy Commission of ICC (hard working team ready to act and influencing others)
  - Internet Governance Forum
  - World Trade Organization (WTO)
<table>
<thead>
<tr>
<th>Some Concepts in Cyber Crime Ontology</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Criminal <strong>Activity</strong></td>
</tr>
<tr>
<td>• Evidence of Motif</td>
</tr>
<tr>
<td>• Evidence of Intention</td>
</tr>
<tr>
<td>• Evidence of Involving</td>
</tr>
<tr>
<td>• Violated <strong>Regulation</strong></td>
</tr>
<tr>
<td>• Consequences</td>
</tr>
<tr>
<td>• Forgiving Condition</td>
</tr>
<tr>
<td>• Filing and Recording</td>
</tr>
<tr>
<td>• Social Treatment</td>
</tr>
</tbody>
</table>
Regulations in Cyber Crime Ontology

• Violation of Regulations:
  • Different in nature types of cyber crime grouped together in a category as violations of a specific single regulation,
  • The same cyber crime type replicated in other categories as it is the violation of the other regulation too,
  • Problem of referring to a cyber crime when the related regulation does not exist in other region(s)
  • Infinite set of cyber crime types as a regulation might be (theoretically) violated in infinite number of ways
  • Complexity of joint international cyber crime tracking as the regulations may differ in each location.
Activities in Cyber Crime Ontology

• Ontology of Activities:
  • Communicate internationally with precise reference to the cyber crime instance,
  • Explain the cyber crime itself without being bound to local regulations,
  • Inform countries about the necessary regulations targeting a specific type of cyber crime of course with priority,
  • Help the global market to gain with more safety in existing and next generation networks,
  • Easier tracking of cyber crime (forensics) as largely invested detection systems will work globally.
Standardization along with Development

- Standardization After Development
  - Modifying the Existing Ontology
  - Using Different Tools
  - Standards ONLY for Ontology Language
- Standardization along with Development
  - A Standard (UI) Development Environment
  - A Shared and Networked Contribution
  - Easily Importing the other Required Ontology
Required Support Areas

- **Supported Management**
  - An Impartial International Entity
  - Always Ready Assigned Members
  - Milestone and Progress Monitoring
  - Running Accessible Servers

- **Financial Support**
  - Writing and Maintenance of Open Source Project
  - Computing Power for Servers and Bandwidth
  - Validation & Verification for Added parts of Ontology

- **Scientific Support**
  - Scientific Evaluation of the Architecture and Process
  - Contribution in the Local Ontology in Research Projects
  - Evaluation of the Ontology in Progress
Estimated Support Costs

- **Management Support**
  - The standards organization accepts to be the management entity
  - Assigning the project Moderator (by standards organization)
  - Project Scheduling and progress reporting by Moderator
  - Setting Up the Servers and Software in a sponsor’s site

- **Financial Support (About € 400,000 in 18 Months)**
  - Six months to Release of Software: Still € 90,000 to spend.
  - Installation and Setup: € 15,000
  - Yearly Site and Software Maintenance man power: About € 60,000
  - Hosting: From € 500 to 6,000 yearly (€ 5,000)
  - Ontology Development in one year: € 150,000
  - Ontology Verification in 4 periods 3 months each with Euros 20,000 payments (all after software release and € 80,000 in total)

- **Scientific Support**
  - Joint Academic Teams from Universities and Research Centers
  - Ontology Development Research Projects based on Software Platform
  - Ontology Evaluation Research Projects