FloraGuard
Tackling the illegal trade in endangered plants

Dr Stuart E. Middleton
University of Southampton
Electronics and Computer Science
Better understanding of the Internet-facilitated online trade in endangered plants.

Better understating of law enforcement challenges and needs.

Develop and test a digital resource to assist law enforcement, researchers and other relevant stakeholders.
Introduction to AI

Definitions

- Artificial Intelligence (AI) >> Machines that learn or problem solve
- Natural Language Processing (NLP) >> Machines that process natural text or speech
- Machine Learning >> Machines that given a task and eval metric learn from experience
- Socio-Technical >> Machines and humans in the loop

AI Landscape around cybercrime research

- Image/Video >> Facial recognition; Object and activity detection
- Audio >> Audio event detection
- Text >> Author attribution and profiling; Information extraction;
- Data >> Social network analysis; Data mining; Predicting policing
- Socio-technical >> All of the above plus Visualization; Interaction; Summarization
Cyclic methodology

- Human in the loop with AI tools
- Cycles
  - Criminology analysis
  - Information extraction
  - Visualization
- Refine final intelligence package
Criminology Analysis
- Subject matter expert >> Lexicon (species, trade jargon)
- Criminologist >> Manual browsing and behaviour coding
- Posts about illegal trades and CITES permits
- Subcultural examples of relevant forum user behaviour
- Coding of posts using NVivo >> Update target suspect lists
- Browsing >> Update web domain lists

Web Search
- Keywords >> Microsoft Bing >> Web pages + domains
- Find search page >> Domain + Entry URI

Crawler
- DARPA MEMEX Undercrawler
- Domain + Entry URI >> Template >> Crawl >> HTML x 10,000’s

Parser
- Python3 app using html.parser and/or bs4
- HTML >> XPath pattern >> Text & Metadata (author, date ...)

Insights from the exploration cycle can be added to the data at any stage of the investigation. This may include new key words, websites and species of interest generated by a combination of criminology analysis, ICT data extraction and conservation science advice.
Step-by-Step Guide

Information Extraction
- Text >> Stanford CoreNLP >> Named Entities
- Named Entities (NE)
  - Person, Location, Time, Org, Species ...
  - People, Objects, Locations, Events (POLE)

Directed Named Entity (NE) Graph
- Text, Metadata, NE >> Directed Acyclic Graph (per target)
- Discussion thread preserves conversation context

Person (target suspect X)

Post A (thread 'buy and sell')

NE (species 'ariocarpus')

Post B (thread 'buy and sell')

Post C (thread 'buy and sell')

Organization (vendor Y)

Insights from the exploration cycle can be added to the data at any stage of the investigation. This may include new keywords, websites and species of interest generated by a combination of criminology analysis, ICT data extraction and conservation science advice.
Step-by-Step Guide

Visualization
- $N \times$ target suspects >> $N \times$ Directed NE Graphs
- Python matplotlib & networkx >> Visualization
- Colour coded node types (people, places ...)
- Up to 400 entities on each graph
- Zoom, Pan, Save image to file

Start a new cycle ...
- Visualization >> Criminology Analysis
- Refine Targets >> Crawl / Graph / Viz

... until results are judged good enough

Intelligence package
- Criminologist prepares summary of evidence
Intelligence output >>
DAG, depth 2
root node target suspect

Target (suspect)
Posts (pseudonymized)
Species
Trade
Location
Organisation
Open-access Software Tools

- Intelligence Graph Visualization
  [https://github.com/stuartemiddleton/intel_viz_entity_graph](https://github.com/stuartemiddleton/intel_viz_entity_graph)

- DARPA MEMEX Undercrawler
  [https://github.com/TeamHG-Memex/undercrawler](https://github.com/TeamHG-Memex/undercrawler)

- Stanford CoreNLP
  [https://stanfordnlp.github.io/CoreNLP](https://stanfordnlp.github.io/CoreNLP)

- Example of a team makeup
  Criminology/Conservation expert + Computer Science intern + software tools
Key Results

Target suspects were mostly found hiding in the long tail of forums

NE graph visualization best for people and locations

Socio-technical AI methodology

- Scale up analysis with AI >> Review orders of magnitude more suspects and POLE entities
- Human in the loop >> Check automated results, look at context, make judgements
Data: Surface and dark web, but not deep web
- Deep web pages are computed from databases on the fly
- Hard to index by search engines, so forum / marketplace posts might be missed

Legal: NE graph evidence ready for a court of law? Not on its own
- It could be used to support target-focussed evidence packages though, with input from criminologist and maybe some relevant out of band corroborating evidence

AI: NLP can find potential suspects but human analysis needed to check suspects
- Socio-technical cycles work >> NLP + human criminological analysis
- Human in the loop AI >> Deep learning NLP where human is part of the model training method
- Wider applications >> Multi-lingual cybercrime forums (hacking, malware), online harms (cyberbullying), community moderation (trolling), disinformation (fake news bot detection)
Open Source Content

Website T&C's
- Public web search >> Find open content without login or signing website T&C's
- Websites login T&C >> Each website T&C's needs a detailed read (crawling, use, research)
- Social media API >> Facebook, Twitter, YouTube etc. >> API's come with rate limits and T&C's

Law enforcement only use open source content (unless they have a warrant)
- We follow a similar approach, avoiding private groups where a deceptive study would be needed
- This limits the coverage we can achieve for our analysis
Images and videos are a minefield - avoid if you can

- We kept crawling to text and metadata only
- It is illegal in UK to store certain types of images (e.g. child abuse images) even accidentally
- Mental health for researchers >> images and videos can be disturbing (duty of care to staff)

Personal data captured when crawling

- Public web pages have made content manifestly public
- Personal data >> impossible to avoid crawling personal data; can pseudonymize analysis results
- Special category data >> limit accidental download by manual choice of websites to crawl
- Manual analysis provides an opportunity to flag up (and remove) special category data
- Ethical approval for study >> University ethics review panel for each study

GDPR and DPIA covered in next section (David Whitehead - Kew)
Pseudonymization and anonymization

- Browsed HTML cannot be pseudonymized (metadata too complex to remove personal data)
- Manual analysis results can be pseudonymized manually (after analysis usually)
- Crawled HTML cannot be pseudonymized (metadata too complex to remove personal data)
- JSON parsed content cannot be pseudonymized (10,000+ volume too large to manually check)
- NE graphs cannot be pseudonymized (removing personal data defeats the purpose of analysis, which is focussed on people engaging in illegal wildlife trade)
- Visualizations and infographics can be pseudonymized for publication (e.g. hash usernames)
- Statistical summaries of datasets can be anonymized

Not perfect >> Search/replace for names; Regex; NER models for PERSON type
UK Ethics panels >> 98% pseudonymized is not pseudonymized is a typical view
Training (law enforcement) on the future use of AI tools

- Formal AI reviews for deployments
- Help decision makers understand both the capabilities of AI and its capacity for error/bias (e.g. understanding if there is training set bias in AI tools being deployed).
- Collaborations with independent academic researchers to advise on AI reviews
Dr Stuart E. Middleton
University of Southampton, Electronics and Computer Science

cr: sem03@soton.ac.uk
web: www.ecs.soton.ac.uk/people/sem
twitter:@stuart_e_middle

FloraGuard: http://floraguard.org/

This work was supported by the Economic and Social Research Council (ES/R003254/1)
Reflections on web crawling techniques from a conservation science perspective

David Whitehead
Royal Botanic Gardens, Kew
CITES@kew.org
Many plants are illegally harvested and traded online. Plant poaching is leading to local or species extinctions.
Challenges include:

- Online anonymity
- Avoidance of border controls
- Spans legal jurisdictions
- Volumes of online content
- Online privacy considerations
<table>
<thead>
<tr>
<th>Species Names</th>
<th>Excluded terms</th>
<th>Buy/sell terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ariocarpus</td>
<td>seed</td>
<td>web+buy</td>
</tr>
<tr>
<td>Ariocarpus+agavoides</td>
<td>seeds</td>
<td>internet+buy</td>
</tr>
<tr>
<td>Ariocarpus+bravoanus</td>
<td></td>
<td>buy</td>
</tr>
<tr>
<td>Ariocarpus+hintonii</td>
<td></td>
<td>buy+online</td>
</tr>
<tr>
<td>Ariocarpus+kotschobeyanus</td>
<td></td>
<td>order</td>
</tr>
<tr>
<td>Ariocarpus+kotschubeyanus</td>
<td></td>
<td>sale</td>
</tr>
<tr>
<td>Ariocarpus+kotschobeyanus</td>
<td></td>
<td>selling</td>
</tr>
<tr>
<td>Ariocarpus+kotsch</td>
<td></td>
<td>purchase</td>
</tr>
<tr>
<td>Ariocarpus+confusus</td>
<td></td>
<td>live plant</td>
</tr>
<tr>
<td>Ariocarpus+albiflorus</td>
<td></td>
<td>swap</td>
</tr>
<tr>
<td>Ariocarpus+retusus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ariocarpus+scaphirostris</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ariocarpus+scapharostroides</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ariocarpus+scapharostrus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ariocarpus+trigonus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tamaulipas living-rock</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tamaulipas living rock</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nuevo leon living-rock</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nuevo leon living rock</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Common misspellings / alternative spellings can be included.

Examples of Latin and Common names for species of interest.


“All data are people, unless proven otherwise”

Zook et al, Ten simple rules for responsible big data research, PLOS Computational Biology, 2017

“Paphiopedilum canhii is now an endangered species with a precarious future. And there we have it: extinction at the speed of the Internet”

Averyanov et al, Field Survey of Paphiopeilum canhii: From discovery to extinction, 2014
Planning an online investigation

• Institutional context
• Perform a risk assessment
• Digital Protection Impact Assessment (DPIA)
The why, what, where and how of your data collection.

What categories of data will you be collecting, or could potentially collect?

What are your legitimate interests for collecting the data?

Seek specialist IT advice on hardware/software.

Templates and advice available at ico.org.uk
Risk Mitigation

- AI limited to carefully selected open-source domains (avoids unintended domains).
- Use AI to anonymise data at source, with one-way hashing (with error).
- Manually remove any other unwanted personal data before analysis; avoid downloading images.
- Develop a Data Management Plan with procedures for Storing; Sharing; Processing; Archiving and Deleting data.
- Collaboration agreements between organisations detail data handling responsibilities.
- Duty of care to researchers, including researcher safety, and effects of encountering certain types of online content.
- Consult data protection officers and legal experts.
- Allow time to factor these processes in.
How to build capacity?

• Multi-disciplinary teams

• International partnerships must meet adequacy requirements under UK law.

• Training conducted using simulated IWT data.
General Discussions

Describe your forum category. Engage your audience and entice them to continue reading.

Dora the unicorn.
Bob Jacobs - Discussion

Need advice please!
Desperate housewife - Discussion

Unicorn Spectacular Show
Unicorn Puffery - Discussion

Unicorn birthday present?
Rainbowmum - Discussion
Thank you! To get in touch, please email: CITES@kew.org

Some references we have found useful:

- Information Commissioner’s Office, ico.org.uk.
- Social Data Lab – socialdatalab.net