Using the *Profitable Biodiversity* Consultancy to Curb Wildlife Trafficking

Timothy C. Haas, Director
Profitable Biodiversity,
https://profitablebiodiversity.com, haas@uwm.edu;
Emeritus Associate Professor (Statistics)
Sheldon B. Lubar College of Business,
University of Wisconsin-Milwaukee,
https://sites.uwm.edu/haas/;
and
Industrial Affiliate
Department of Computer Science, UCLA

Figure 1: The Bengal tiger has been poached to near extinction for its bones and genitals.

This business brief helps executives to quickly see how a firm can make money operating a wildlife trafficking investigations project. A *biodiversity offering* that has a *biodiversity premium* as part of its purchase price, is purchased by a *biodiversity-concerned customer*. This premium funds a *biodiversity project* that here, takes the form of a confederation of wildlife crime investigators across the world who contribute to a wildlife cybercrime intelligence database. Queries against this database support the efforts of confederation members to build cases against individuals who commit wildlife crimes. Successful prosecutions supported by such evidence put these criminals out of business and bring them to justice. Doing

so is crucial because stopping wildlife trafficking is the most important step towards preserving the earth's biodiversity.

Another business brief available at `www.profitablebiodiversity.com/busbriefgen.pdf` fleshes out this new profit-driven approach to sustaining biodiversity.

A Wildlife Trafficking Investigations Project

Definitions

Any individual engaged in the illegal and physical acquisition of plants, animals, or animal body parts through the poaching (digging up, cutting, shooting, trapping, or poisoning) of live plants or animals is referred to here as a *poacher*. Poachers; middlemen who sponsor poaching raids; and those criminals who arrange shipments of poached plants, animals, or animal body parts are all *traffickers*. Traffickers are often members of some particular *wildlife trafficking syndicate* (WTS) [3]. Syndicate members are typically called *players*.

The offering and attached project

This brief describes a hypothetical biodiversity offering that takes the form of an insurance policy. A portion of the revenue from this policy's sales funds a wildlife trafficking investigations project through the following technologies.

1. A distributed, federated, peer-to-peer (P2P) database of wildlife traffickers and their transactions [3]

2. Advanced marketing analytics to both gauge the success of a new biodiversity offering and predict the likelihood of repeat purchases

3. A predictive model of the political-ecological system that includes interactions between the WTS and the wildlife traffickers investigations project

4. An Internet of Things (IoT)-based monitoring program of this system

5. A *biodiversity dashboard* that displays this stream of monitoring data in real time

These technologies are contained in the *Intel Kit* that is available at [4]. This kit is engineered to help firms operate a wildlife trafficking investigations project supported by a wildlife cybercrime intelligence database. As mentioned above, a firm funds this project through sales of an attached and profitable biodiversity offering [1, 18].

The Wildlife Trafficking Crisis

Only a small proportion of trafficked wildlife is seized by authorities [3]. This suggests that current efforts at investigating and prosecuting wildlife traffickers needs to be increased by at least one order of magnitude. Such a global increase in investigations and prosecutions may only be possible if the resources of the private sector are brought to bear on this ongoing slaughter.

Wildlife trafficking transactions occur mainly over the internet and mobile phone networks [3]. An international database run by investigators living in different countries is needed to help de-duplicate trafficker identities and to share criminal intelligence so that by putting these criminals out of business, the ongoing slaughter of wildlife can be slowed down. Doing so may be the only hope for most of the planet's endangered species. But these investigators are all peers in that no one country can force investigators in other countries to share their intelligence.

One solution to this intelligence-sharing problem is to create a P2P wildlife cybercrime intelligence database that is maintained by a *confederation* of criminal intelligence analysts across several countries.

A Wildlife Cybercrime Intelligence Database

Database entities

The confederation's wildlife cybercrime intelligence database consists of both open access data and secure intelligence acquired by confederation members during the course of their investigation and surveillance operations. As presented in [3] and [5], database entities are players, phone calls, bank accounts, vehicles, firearms, wire transfers, and *wildlife shipments*. Such shipments can consist of live plants, live animals, plant parts, or animal body parts, e.g. tiger bones.

Attributes of these entities include

1. Players: Personal information including their names, addresses, and phone numbers
2. Phone calls: Caller, callee, and conversation transcript
3. Bank accounts: Account numbers involved in wire transfers between players
4. Vehicles: Owner, and registration number
5. Firearms: Owner, and serial number
6. Wire transfers: Date, originator, destination, and amount

7. Wildlife shipments: Date, origin location, destination location, contents, and amount

Queries

Typical queries to this database include:

1. Calls wherein the transcript contains the word "poaching"
2. Calls wherein the transcript contains the word "price, deal, animal body part"
3. Trafficker arrests: date; charges; and a list of seized contraband
4. The where; when; and size of wildlife shipments through time

Detecting insider attacks

Insider attacks can cause major problems for military/terrorism/criminal intelligence systems. Recent examples include then-President Trump's sharing of Israeli intelligence with the Russians [6], and the attacks carried out by Edward Snowden, Chelsea Manning, and Nghia Hoang Pho [7]. Detecting such individuals is challenging within a hierarchically controlled database but is even harder to achieve in a P2P database.

Reference [3] offers one way to manage a P2P database but offers only an investigator-initiated way to detect whether a particular confederation member is an insider threat plus a voting-based way to corroborate an investigator's accusation against such a confederation member.

Modern *insider threat detection* algorithms, however, watch a database user's pattern of queries against the database and when this pattern changes, this user is declared to be a threat. Although these *within-database* methods of detecting insider attacks can be automated, they have a shortcoming in that they are not useful at detecting those users who may become a threat in the near-future. To do this, the monitoring of a user's personal finances, contacts, and ideally, evidence of the user accepting bribes can help prevent insider attacks rather than merely detecting ongoing attacks [3].

Here, insider threats are detected using a modified form of the *data-centric* method of [8]. Specifically, a *modular neural network* (MNN) classifier [9] is used to predict whether a member's query result is *anomalous* or not. If it is declared by the algorithm to be anomalous, this is evidence that this member is using their access to the confederation's database for malicious purposes.

In this wildlife cybercrime intelligence database, each time a member sends a query to the database, an intermediate processor called the *insider threat detector* (ITD) uses a trained MNN to predict the query's author. This is done by presenting the query result's S *vector*

[8] to the MNN and receiving back a predicted query author. If this predicted author is not the actual author, this query is flagged as anomalous and given as evidence that the actual author may be attacking the database. These attack-detection components have been integrated into the P2P *relational database management system* (RDBMS) available at [10].

Marketing Analytics

A biodiversity offering is a new form of a relationship between a firm and a customer. And, the niche market that such an offering will appeal to may turn out to be a surprising demographic [11]. For these reasons, advanced marketing analytics are needed to guide the early tuning of the offering's marketing campaign in order for the offering to reach its maximum sales potential.

An *autoregression* model can quantify the relationship between certain drivers and the potential for sales of a new biodiversity offering. In particular, such a model fitted to purchase data can help identify those consumer groups who are driving sales growth. These groups can be characterized by different combinations of gender, age, income, home ownership, and education level. The SAS^{TM} program, `salesgrowth.sas` available at [10] fits this model to a test data set.

Another model that is needed is one that can predict the likelihood of a repeat purchase of the offering. *Autoregressive logistic regression* models can provide these predictions. The SAS code file, `channels.sas` at [10] fits such a model to a test data set.

These two models are predictive so that once they are fitted to data, they can be used to predict conditions that will lead to future revenue growth of the biodiversity offering.

Example: Saving the Bengal Tiger

Many private firms possess expertise in pursuing financial fraud investigations. For instance, most insurance companies have an in-house *special investigation unit* whose sole purpose is to investigate insurance fraud. Staff within such units include professionals experienced in conducting criminal investigations and forensic accountants skilled in detecting financial irregularities from online sources. Such a firm would be able to assign one of their existing fraud investigation units to a wildlife trafficking investigations project.

Say that a hypothetical insurance firm has chosen a class of auto insurance policies for their biodiversity offering. This firm has identified their biodiversity project to be carrying out ongoing investigations into the trafficking of Bengal tiger body parts. The files in the Intel Kit [4] detail a hypothetical investigation into such wildlife trafficking. These files constitute an extension and completion of the example sketched in [3]. The end result of

these investigations is the sharing of evidence and recommended actions with India's Wildlife Crime Control Bureau and other law enforcement authorities. These recommended actions take the form of three *lists* as follows. The *Detain List* identifies those traffickers who should be immediately detained, the *Surveil List* identifies those traffickers who should be placed under surveillance, and the *Interdict List* details upcoming poaching raids, transport events, and monetary transfers that should be interdicted.

This biodiversity project will require the cooperation of Indian conservation agencies. This cooperation can be won through the services of the firm's *liaison consultant*. References [1] and [18] discuss why this consultant is critical to the success of any in-country biodiversity project such as this wildlife trafficking investigations project. Reference [12] gives a step-by-step guide to setting up a liaison office in India.

To aid their investigations of Bengal tiger body parts trafficking, the firm has voluntarily joined a confederation of wildlife trafficking investigators. This confederation employs a software system that allows confederation members to share among themselves, intelligence on traffickers and their shipments of tiger body parts. The software package that builds this system is available at [10].

Further, this firm has volunteered to maintain the *logistics node* (see [3]) of the confederation's P2P wildlife crime database. This node stores each confederation member's contact information, audit information on each member's trustworthiness, and each database node's ability to maintain cybersecurity. The logistics node also ensures that access to any criminal intelligence held in the confederation's database is managed by the *Global Authorization Derivation* (GLAD) database access control tool [13]. This tool ensures that a single member's security concerns are immediately addressed by all other confederation members.

A model of the tiger-hosting political-ecological system

A model of the political-ecological system that contains the Bengal tiger population and the traffickers preying on them is needed to to allow the confederation to see how their efforts at removing traffickers from the ecosystem are affecting tiger abundance. To this end, this *simulator* computes predictions of tiger abundance as that population responds to the removal of different cadres of traffickers.

The simulator consists of (a) submodels of the decision making of several groups; and (b) a submodel of the tiger-hosting ecosystem. These submodels are as follows.

1. A group of tiger poachers
2. A group of middlemen involved in buying, transporting, and selling tiger body parts
3. Chinese consumers of tiger body parts

4. The Wildlife Crime Control Bureau within India's Ministry of Environment, Forests, and Climate Change (MoEFCC)

5. An individual-based submodel of Bengal tiger abundance in Bandhavgarh Tiger Reserve, India.

Political-ecological actions history data set

The Intel Kit's `polecotigers.dat` file contains observations on political-ecological actions and was acquired using the STAR protocol [18]:

```
comment Political-Ecological Actions Data
comment Date Actor          Action
begin
03-15-11  tigerpoacher1  poach_for_cash
11-05-12  tigerpoacher2  poach_for_cash
07-30-11  wccbureau      arrest_poachers
end
```

The Intel Kit's `obstigers.dat` file contains simulated observations on tiger abundance. In real life, this data would be collected either by contracted field ecologists or through technological methods such a camera traps and/or remote sensing techniques.

These two data sets are combined and used to statistically estimate the values of the simulator's parameters. Once fitted, this simulator is used to predict tiger abundance under different poaching rates that depend on the proposed removal of different cadres of traffickers. The optimal cadre of traffickers is added to the confederation's Detain, Surveil, and Interdict lists as mentioned above.

The social network model of the WTS

In addition to the simulator, the project maintains a social network model of the WTS being investigated [3]. This social network model is integrated with the simulator.

For purposes of computing social network measures of WTS characteristics that are useful to law enforcement, the Intel Kit assumes that the confederation gathers evidence on the WTS at three different times. The first time is to find out the size, connectivity, and assets of the current, undisturbed WTS. The confederation then quietly watches the network for several weeks and at the end of that period, observes its size and connectivity again. As soon as this second set of criminal intelligence has been gathered by the confederation, recommendations are communicated to law enforcement authorities as to those WTS players who should be detained, and those who should be surveilled. Also, recommendations are communicated as to those upcoming WTS actions that should be interdicted. Finally, some

weeks after these arrests and interdictions, the confederation gathers information on the size and connectivity of the recovering WTS. Call these three time points, t_1, t_2, and t_3, respectively. Simulated intelligence on the WTS at each of these time points is contained in the Intel Kit's `tiger_traffickers_syndicate.dat` file.

The Intel Kit's output report file, `tigerintel.txt` contains (a) predictions of those players in the WTS who are predicted to move into leadership roles (called *Rising Stars*); and (b) the resiliency of the WTS. This latter value is a prediction of how long it will take the syndicate to recover its full functionality after having lost several of its players at time t_2. [5].

Monitoring Program

The monitoring program collects and streams to the biodiversity dashboard, real-time values on the number of tiger trafficker arrests, the number of tiger trafficker convictions, the number of seized shipments of tiger body parts, and estimates of tiger abundance in the Bandhavgarh Tiger Reserve, India.

One source of data on the number of arrested tiger traffickers and the status of their subsequent court cases is the Centralized Wildlife Trafficking Investigative Database (CWT-ID) maintained by C4ADS [14]. Access to this data will require setting up a (possibly paid) partnership with C4ADS. Again, courtesy of C4ADS, one source of data on the number of seized shipments of tiger body parts can be freely acquired from [15].

The Reserve's tiger abundance can be estimated by first acquiring tiger sightings data at different time points from (say) India's National Tiger Conservation Authority [16]. The firm's liaison consultant would work with the National Tiger Conservation Authority to secure this *capture-recapture data* for the confederation's P2P wildlife crime database. As an alternative, [17] takes a continuous-time approach to using such data to estimate abundance. A SAS code for computing these abundance estimates along with an accompanying test data set is available at [10].

The Biodiversity Dashboard

Using data streamed from the monitoring program, this dashboard displays real-time values on the number of tiger trafficker arrests, the number of tiger trafficker convictions, the number of detected shipments of tiger body parts, and tiger abundance in India's Bandhavgarh Tiger Reserve. The dashboard consists of four time series plots stacked vertically in the above order.

The JavaFX$^{\text{TM}}$ code that downloads the needed data along with the script that creates

the dashboard's graphics is available at [10]. Figure 2 displays the dashboard generated by these two programs. In this Figure, the convictions, shipment seizures, and tiger abundance time series are hypothetical.

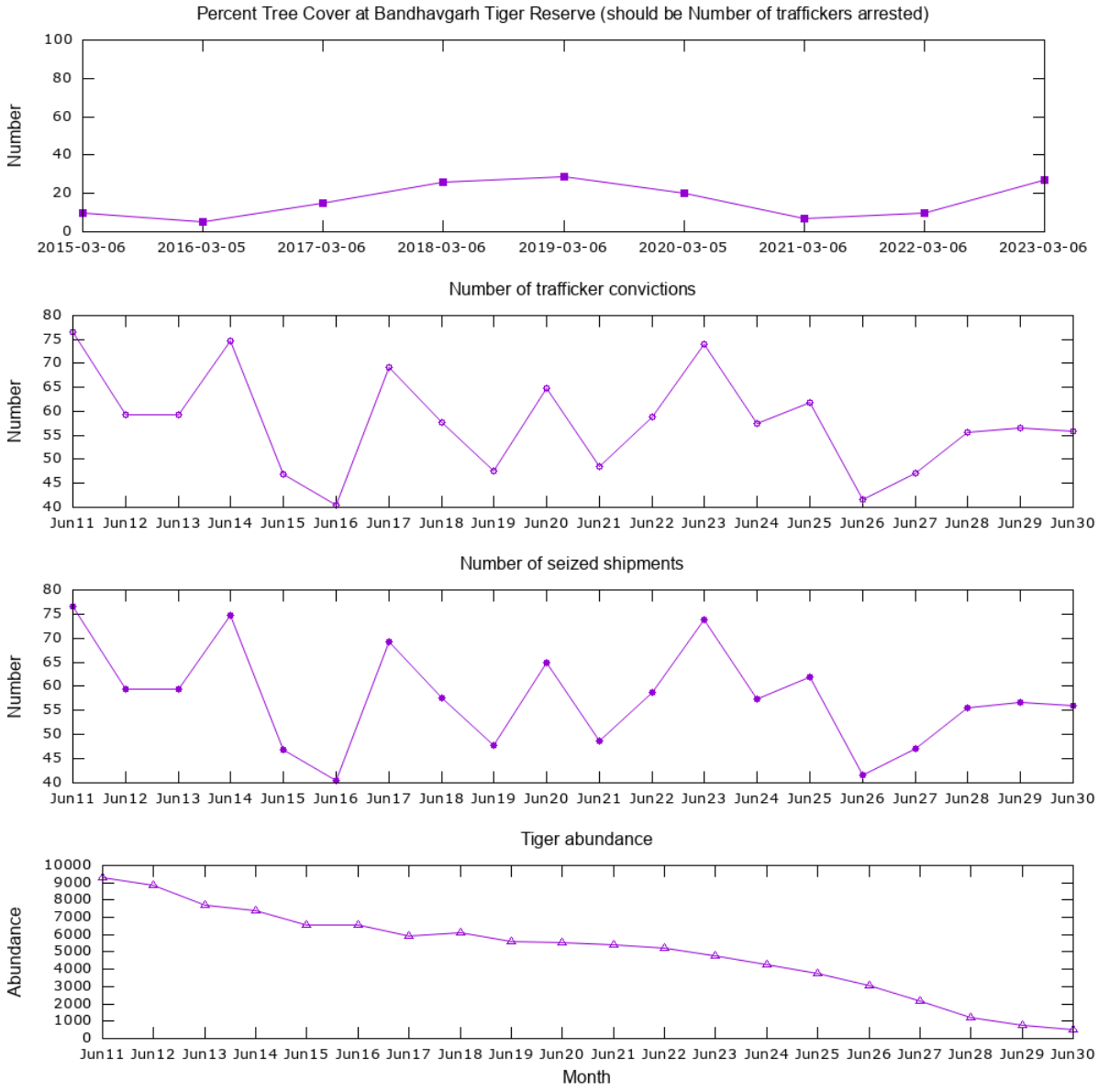

Figure 2: Biodiversity dashboard. An audit information note would be added to the dashboard that might read: `Audit information is available at https://insurance_firm.com/tigers/audit/.`

For purposes of technology development, the JavaFX program, `Inteldash.java` [10] queries the Oak Ridge National Laboratory Web Service API [19] for Percent_Tree_Cover observations taken yearly from 2015 through 2023 at the Bandhavgarh Tiger Reserve, India. This is accomplished by issuing three separate queries to the service:

1. A list of all API-accessible products
2. A list of available dates of the Percent_Tree_Cover product at the Reserve's GPS coordinates
3. A download of Percent_Tree_Cover values in a 1 km square region surrounding this location

This Percent_Tree_Cover variable replaces the number-of-trafficker-arrests variable in Figure 2 simply to show how the provided JavaFX program, `Inteldash.java` can be used to automatically download data from the web at regular time points. As discussed in the Intel Kit's `Monitoring` web page, in actual application, the firm's liaison consultant would work with India's Wildlife Crime Control Bureau to set up a web service to provide an IoT-accessible interface to such number-of-trafficker-arrests data.

The Way Forward

A firm having expertise in criminal intelligence analyses can profitably help to preserve a species of their choice. The time from the start of a biodiversity offering to the time it becomes profitable can be shortened by use of the resources freely available at [4]. For immediate assistance with these tools and with the task of establishing an ecological monitoring program, please send an email to `haas@uwm.edu`.

References

[1] Haas, T. C. (2022), "Profitable biodiversity," *Cogent Social Sciences*, 8(1): 1-24. https://doi.org/10.1080/23311886.2022.2116814 https://www.tandfonline.com/doi/full/10.1080/23311886.2022.2116814

[2] Haas, T. C. (2024), "A new technology-based tool for building profitable biodiversity-conserving offerings," *The European Journal of Sustainable Development,* 13(3): 1-13. https://doi.org/10.14207/ejsd.2024.v13n3p57

[3] Haas, T. C. (2023), "Adapting cybersecurity practice to reduce wildlife cybercrime," *Journal of Cybersecurity*, 9(1): 1-20.

https://doi.org/10.1093/cybsec/tyad004
https://academic.oup.com/cybersecurity/article/9/1/tyad004/7083342

[4] Haas, T. C. (2024) *Profitable biodiversity website.* https://profitablebiodiversity.com.

[5] Haas, T. C. and Ferreira, S. M. (2015), "Federated databases and actionable intelligence: Using social network analysis to disrupt transnational wildlife trafficking criminal networks," *Security Informatics,* 4:1.
https://doi.org/10.1186/s13388-015-0018-8
http://www.security-informatics.com/content/4/1/2
http://www.springer.com/-/4/0d7808225b2a4876986ead314e72ee99

[6] Gramer R. (2017), "Israel changed intelligence sharing with U.S. after Trump comments to Russians," *Foreign Policy*, 24 May.
https://foreignpolicy.com/2017/05/24/israel-changed-intelligence-sharing-with-u-s-after-trump-comments-to-russians/

[7] Raywood, D. (2018), "Top ten cases of insider threat," *Infosecurity Magazine,* 25 December.
https://www.infosecurity-magazine.com/magazine-features/top-ten-insider-threat/

[8] Mathew, S., Petropoulos, M., Ngo, H.Q., Upadhyaya, S. (2010). "A Data-centric approach to insider attack detection in database systems," (in) Jha, S., Sommer, R., Kreibich, C. (eds.) Recent Advances in Intrusion Detection. *RAID 2010. Lecture Notes in Computer Science,* vol 6307. Springer, Berlin, Heidelberg.
`https://doi.org/10.1007/978-3-642-15512-3_20`.

[9] Anand, R., Mehrotra, K., Mohan, C. K., and Ranka, S. (1995), "Efficient classification for multiclass problems using modular neural networks," *IEEE Transactions on Neural Networks,* 6(1): 117-124, January. doi: 10.1109/72.363444.

[10] Haas, T. C. (2024) *Profitable biodiversity software.* https://profitablebiodiversity.com/software/index.html

[11] Zhu, T., Liu, Y., Tang, Q., and He, J. (2022), "Identifying and modeling the dynamic evolution of niche preferences," *Electronic Commerce Research and Applications,* 52, 101117, https://doi.org/10.1016/j.elerap.2022.101117

[12] Maiervidorno (2024), *When to set up a liaison office in India 2024* https://www.maiervidorno.com/blog/when-to-set-up-a-liaison-office-in-india/

[13] Castano, S. (1997), "An approach to deriving global authorizations in federated database systems," (in) Samarati P., Sandhu R.S. (eds) *Database Security. IFIP Advances in Information and Communication Technology,* Springer, Boston, MA. https://doi.org/10.1007/978-0-387-35167-4_5

[14] C4ADS (2024), *Centralized wildlife trafficking investigative database (CWT-ID)*, C4ADS. https://c4ads.org/wildlife-trafficking/

[15] C4ADS (2024), *Wildlife dashboard*, C4ADS. https://wildlifedashboard.c4ads.org/home/about

[16] National Tiger Conservation Authority (2024), *Tiger abundance data*. (https://ntca.gov.in/monitoring/#monitoring

[17] Ferreira, S. M., Beukes, B. O., Haas, T. C., and Radloff, F. G. T. (2020), "Lion (panthera leo) demographics in the southwestern Kgalagadi Transfrontier Park," *African Journal of Ecology*, 58(2): 348-360. https://doi.org/10.1111/aje.12728

[18] Haas, T. C. (2024). Protocol to discover machine-readable entities of the Ecosystem Management Actions Taxonomy. *STAR Protocols*, Cell Press, Elsevier, 5(2), 103125: 1-12. 10.1016/j.xpro.2024.103125

[19] Oak Ridge National Laboratory (2024), *Web service API*. https://modis.ornl.gov/data/modis_webservice.html