Sustaining Biodiversity with an Insider-Threat-Resistant Wildlife Cybercrime Investigation Tool

Abstract

Wildlife trafficking is driving many species to extinction. Most of these transactions are conducted over the internet and mobile phone networks. This article describes a new software tool that can effectively support an international confederation of criminal intelligence analysts in their efforts to curb wildlife trafficking. This tool consists of three modules: A federated, wildlife cybercrime intelligence database system; a political-ecological system simulator; and a social network model of the wildlife trafficking syndicate under investigation. The database module receives predictions of local extinction risks on the species being conserved that have been computed by a credible model of the species-hosting political-ecological system. The confederation integrates these predictions with a social network analysis in order to identify those traffickers who are associated with regions having high local extinction risks. This new approach to conducting a wildlife trafficking investigation is illustrated by finding a hypothetical trafficker who is most responsible for the decline of the East African cheetah (*Acinonyx jubatus*) population. This integration of a wildlife cybercrime intelligence database, a credible model of a species-hosting political-ecological system, and a social network model of a wildlife trafficking syndicate is not only new, but is also the future of effective wildlife trafficking investigations. This article also delivers a new solution to the open problem of how to guard a database against insider attacks. This solution is optimized for use in a peer-to-peer, nonhierarchically-managed database system such as the one described herein. A simulation study shows this new insider threat detection algorithm is effective at detecting individuals with access to a secure database who have unfortunately, gone rogue.

Abbreviations:

CA: Consistency Analysis
FWCIDMS: Federated Wildlife Criminal Intelligence Database Management System
GLAD: Global Authorization Derivation
ITD: Insider Threat Detector

KWS: Kenya Wildlife Service
NGO: Nongovernmental Organization
SIU: Special Investigation Unit
SQL: Structured Query Language
TAWA: Tanzania Wildlife Management Authority
WCITS: Wildlife Cybercrime Investigation Tool
WTS: Wildlife Trafficking Syndicate

1 Introduction

Any individual engaged in the physical acquisition of animals/plants or their parts through the poaching (shooting, trapping, poisoning, digging) of live animals/plants is referred to here as a *poacher*. Poachers, those middlemen who sponsor poaching raids, and those criminals who arrange shipments of live animals/plants or their parts are all *traffickers*. These traffickers often belong to a particular *wildlife trafficking syndicate* (WTS) (Haas 2023). When such a syndicate is modeled as a criminal network using social network theory (Haas and Ferreira 2015), the criminals who belong to the syndicate are referred to as *players*.

1.1 Using criminal intelligence to curb wildlife trafficking

Wildlife trafficking transactions occur mainly over the internet and mobile phone networks. An international database run by criminal intelligence analysts living in different countries is needed to help de-duplicate trafficker identities and to share intelligence so that these criminals can be put out of business and brought to justice. This may be the only hope for most of the planet's endangered species of flora and fauna (Haas 2023). One way to form such a shared, international wildlife crime intelligence database is to create a peer-to-peer (P2P) criminal intelligence database that is maintained by a *confederation* of criminal intelligence analysts who are employed across several countries. Haas (2023) develops an early form of such a database. Assume that this confederation has preselected a particular species to be the focus of their wildlife trafficking investigations. The success of this confederation's wildlife trafficking investigations is inversely proportional to the temporally-discounted risk of the preselected species' global extinction (hereafter, *extinction risk*). To succeed then,

criminal intelligence analysts need to focus their investigations on those traffickers who are associated with regions that carry the highest local extinction risks of the preselected species. This is because if a species is everywhere locally extinct, it is globally extinct.

To this end, this article describes a *wildlife cybercrime investigation tool* (WCIT). A WCIT consists of three modules: a *federated, wildlife cybercrime intelligence database management system* (FWCIDMS); a *political-ecological* model and simulator of the system that hosts the preselected species; and a social network model of the WTS built from the intelligence held in the FWCIDMS

Output from simulation runs of the political-ecological model (hereafter, the *simulator*) includes the local extinction risk for each region within the political-ecological system's spatial extent. Then, using a social network analysis of the traffickers associated with regions carrying high extinction risks, the confederation creates three lists: A list of those players who should be immediately arrested, called the *Detain list*; a list of those players who should be surveiled, called the *Surveil list*; and a list of those near-future trafficking actions that should be interdicted, called the *Interdict list* (Haas 2023).

The WCIT described herein is new.

1.2 Article deliverables and layout

This article delivers the following.

1. A tool for investigating the trafficking of a preselected species that is informed by a *credible* (Haas 2020, Haas 2024a) model of the political-ecological system that hosts that species;

2. An FWCIDMS that is a synthesis and extension of both the political-ecological database of Haas (2021) and the federated wildlife cybercrime intelligence database of Haas (2023);

3. An automatice procedure embedded in the FWCIDMS for detecting insider attacks against it;

4. A demonstration of the WCIT being used to help conserve the East African cheetah (*Acinonyx jubatus*) population.

The FWCIDMS is described in Section 2 along with its built-in procedure for detecting insider threats. The use of simulator output and social network analysis to identify players to detain or surveil along with WTS actions to interdict is detailed in Section 3. As an example, the WCIT is applied in Section 4 to the conservation of East African cheetah. Issues surrounding this tool are discussed in Section 5. Conclusions are drawn in Section 6.

All JAVA^{TM} code needed to build the WCIT is available in this article's Supplementary Files; in the `Software` section of the *Intel kit* (Haas 2025c); and at a Dryad repository (**would be purchased by the author if this manuscript is accepted and assigned a DOI**). The input files needed to run this article's example are included at all of these locations.

2 The FWCIDMS

2.1 Nomenclature

A *relational* database consists of observations (records) on *entities*. An entity is a particular object or event in the real world. These entities are characterized by their *attributes* (Haas 2023). A *query* against a database is a request from a user to add to the database, delete from the database, or copy from the database – a set of records concerning selected entities and the values of selected entity-specific attributes. A query produces a *query result*. This result can contain many records of entity attribute values. Here, a bundle of query results where each query result is generated from a separate query, is referred to as a *set of query results* rather than simply *query results* in order to sharply distinguish a collection of query results from the (possibly) many records inside one particular query result.

2.2 Database entities

An FWCIDMS consists of both open access data and secure intelligence acquired by confederation members (hereafter, simply *members*) during the course of their investigation and surveillance operations. Extending Haas and Ferreira (2015) and Haas (2023), database entities are `Players`, `Phone Calls`, `Vehicles`, `Firearms`, `Bank Accounts`, `Wire Transfers`, `Wildlife Product Shipments`, and `Arrests`. Shipments can consist of live animals/plants or their parts, e.g. tiger bones.

Attributes of these entities are listed in Table 1.

Entity	Attributes	Scale
Player	name	nominal
	town	"
	country	"
Phone	owner	"
	phone number	"
Link	from-player	"
	to-player	"
Vehicle	owner	"
	registration number	"
Firearm	owner	"
	serial number	"
Bank account	owner	"
	account number	"
Wire transfer	originator	"
	receiver	"
	amount	continuous
Wildlife product	origin	nominal
shipment	destination	"
	product type	"
	size	continuous
Arrest	player	nominal
	date	continuous
	arresting authority	nominal

Table 1: Entities and their attributes contained in the FWCIDMS. Most of these attributes are nominally-valued.

2.3 Queries

Typical queries to this database would include:

1. Phone calls wherein the call's transcript contains the word "poach"
2. Calls wherein the transcript contains the word "price, deal, animal/plant part"
3. The where, when, and size of wildlife shipments over a designated time interval.
4. Trafficker arrests: date, charges and what was seized, e.g. wildlife products, phones, firearms, and/or vehicles.

2.4 Database access privileges

The *logistics node* of the FWCIDMS (Haas 2023) stores each member's contact information along with auditing and security information on each database node. This node also manages membership dues, and controls database access with the Global Authorization Derivation (GLAD) protocol (Castano et al. 1997). The GLAD protocol has been adapted by Haas (2023) for use in a federated cybercrime intelligence database. The use of GLAD ensures that a single member's security concerns are not dismissed by a cadre of other members (Haas 2023).

2.5 Protecting a database from insider threats

Members are all peers. This means that members in one country cannot force members in other countries to share their criminal intelligence by uploading it to the FWCIDMS. Conversely, once uploaded, each member can only *trust* other members to not access their uploaded data for malicious purposes and/or damage such data. Hence, such a database management policy begs the question: Why should one criminal intelligence analyst in one country, trust another who lives in some other country and for whom they know nothing about? Indeed, a member might be bribed or blackmailed into using their database access privileges to *attack* the criminal intelligence database itself. Such attacks can take many forms including (a) the downloading of data with the intent to distribute it to the very criminals the confederation is gathering evidence on, or (b) the editing of database entries with the intention of undermining investigations. These member-attack potentialities are called *insider threats* (Kul et al. 2020).

Zero trust database access safeguards (Wang et al. 2025) do not apply to this case because members already possess GLAD-determined database access privileges.

Agencies within the United States government have a similar problem: How to enable the sharing of military/terrorism intelligence with intelligence agencies in other countries? These foreign intelligence specialists do not work for the United States and are under no compulsion to cooperate with United States intelligence specialists. For military/terrorism intelligence systems, in particular, insider attacks can cause serious damage. Recent examples include then-president Trump's sharing of Israeli intelligence with the Russians (Gramer 2017), and the attacks carried out by Edward Snowden, Chelsea Manning, and Nghia Hoang Pho

(Raywood 2018).

Detecting those insiders who launch these attacks is challenging within a hierarchically controlled database running under a *role based access control* (RBAC) policy (Marquis 2024). In RBAC, each member is assigned a particular role that has associated with it, a fixed set of database access privileges. But in the federated wildlife cybercrime database of Haas (2023), all members have the same role and their database access privileges are automatically controlled via GLAD.

As highlighted in Haas (2023), this lack of differentiated roles means that an international wildlife cybercrime intelligence database requires different cybersecurity solutions than those typically installed in corporate or governmental databases wherein database access is determined and enforced through a strict hierarchy of organizational authority. To address this vulnerability of a role-free database, this article describes a tested *insider threat detector* (ITD) that makes an FWCIDMS resistant to attacks by its own members.

2.5.1 Challenges and previous work

A confederation's FWCIDMS, being shared by peer criminal intelligence analysts who reside in many different countries, can be vulnerable to insider attacks. This vulnerability will be recognized by any criminal intelligence analyst who might be thinking of becoming a member of such a confederation. Therefore, the database needs to have in it, a system for safeguarding itself from such attacks. With the nonhierarchical control of the database and the voluntary nature of being a member of it, such safeguards need to be convincing to both current and potential members. Otherwise, those very criminal intelligence analysts who could contribute the most to the fight against wildlife trafficking will hesitate to join the confederation since by doing so, they may see their highly confidential criminal intelligence stolen or corrupted by any number of rogue members. In other words, a confederation will only be effective at curbing wildlife trafficking if its FWCIDMS is running an insider threat detection technology that is capable of detecting members who have gone rogue.

Haas (2023) offers one way to manage a federated P2P database but offers only a member-initiated way to detect whether some other member is an insider threat. Once a member claims another member is an insider threat, Haas (2023) can only offer a voting-based way to corroborate this member's accusation.

In contrast to this member-initiated approach, modern insider threat detection algorithms watch a member's pattern of queries or query results and when these patterns change, this member is declared by the algorithm to be a threat. These *within-database* methods of detecting insider attacks can be made part of the automatic functioning of an FWCIDMS.

2.5.2 ITD algorithm

Here, insider threats are detected using a modified form of the *data-centric* method of Mathew et al. (2010). Specifically, a *modular neural network* (MNN) classifier (Anand et al. 1995) is used to predict whether a member's query result is anomalous or not. If it is declared to be anamolous, this is taken as evidence that this member is using their access to the confederation's database for malicious purposes.

In the FWCIDMS, each time a member sends a query to the database, the ITD uses a trained MNN to predict the query's author. This is done by presenting the query result's *S vector* (Mathew et al. 2010) to the MNN and receiving back, a prediction of the query's author. If this predicted author is not the query's actual author, this query is flagged as anomalous and given as evidence that the actual author of the query may be attacking the database.

This ITD is new.

2.5.3 Training the ITD

A data set containing a set of query results from each of the confederation's r members is used for train the MNN where the number of the MNN's modules is set to r. This means that each neural network module will become a specialist at recognizing query results from its assigned member. The Quasi-Newton-based algorithm of Setiono and Hui (1995) is used to fit the MNN's parameters to the training data set. The objective function consists of averaged prediction error rates for each member. Doing so eliminates the data imbalance problem wherein some members submit fewer queries to the database than other members.

A modified S vector is used to form summary measures on the attribute values contained in a query result. For this to work, each attribute on each entity in a query result needs to be uniquely identified because attributes are specific to the entity that they describe (Table 1).

Let n_d be an entity's total count (tally) in the database. Let $n_i^{(m)}$ be the tally of this entity in the i^{th} query result. In the database, arbitraily index the unique values of a particular discretely-valued attribute owned by a particular entity with the integers, $\{1,\ 2,\ \ldots,\ n_{att}\}$.

Several entities may have the same value of an attribute. In this case, attribute values may repeat in a query result. For instance, the attribute `country_of_residence` owned by the `trafficker` entity might have the unique values of Kenya, Tanzania, South Africa, Nambia, and Mozambique. These labels might be given the arbitrary index values of 1, 2, 3, 4, and 5, respectively. This yields $n_{att} = 5$. A query result might contain $n_i^{(m)} = 7$ occurrences of the `trafficker` entity with `country_of_residence` attribute values of: {South Africa, Tanzania, South Africa, Kenya, Mozambique, Mozambique, Mozambique}. The index values in the query result would therefore be $\{3,\ 2,\ 3,\ 1,\ 5,\ 5,\ 5\}$ or, in sorted order, $\{1,\ 2,\ 3,\ 3,\ 5,\ 5,\ 5\}$. It is emphasized that n_{att} is unrelated to n_d. For instance, in the above example, the number of trafficker entities in the database might be large, e.g. $n_d = 275$.

Attributes may be nominally-, ordinally-, or continuously-valued. The next Section shows how each of these scales is transformed into variables that are suitable for inclusion in the MNN's input vector.

2.5.4 Summary statistics for attribute data

If the attribute is nominally-valued, an arbitrarily assigned but unique index value is given to each label of such an attribute as it is initially read into the database. These index values allow a nominally-valued attribute to have S vector measures assigned in exactly the same way as a true, ordinally-valued attribute such as the number of vehicles owned by a trafficker. Therefore, it suffices to consider only an ordinally-valued attribute.

Say that such an attribute has n_{att} unique values in the database. For instance, the attribute, `name` of a `trafficker` entity will have almost as many unique values as there are unique individual trafficker entities in the database. The histogram of such a nominally-valued attribute in a query result would most likely have exactly one observation in each histogram bin when a bin is defined to be a single, unique attribute value. For such an attribute, a histogram does not convey useful information about the nature of a query result. A criminal intelligence database, however, focuses on individuals and their characteristics. Such databases will typically contain many entity-attribute relationships wherein each entity

possesses a unique label of a nominally-valued attribute (Table 1).

Therefore, instead of histogram-based measures, the normalized sample median, normalized sample interquartile range (IQR), and the relative tally of attribute values are used to summarize the ordered index values of an ordinally-valued attribute in a query result. The idea is to use the sample median to locate the attribute, the IQR to measure its dispersion, and the tally to measure its magnitude. How these measures are computed is described next.

The *quantile function*, $Q(p)$ is the generalized inverse of the *cumulative distribution function,* $F(x)$: $Q(p) = \inf\{x : F(x) \geq p\},\ 0 < p < 1$ (Redivo et al. 2023). The quantile function may be estimated in two steps. First, assign an index value to each unique attribute value contained in the database, e.g. assign a unique integer value to each unique string of the `trafficker` entity's `name` attribute. Let $x_1 < x_2 < \ \ldots \ < x_n$ be these ordered attribute index values. Second, employ a well-known quantile estimator to estimate $Q(p)$ from these ordered index values. This quantile estimator works as follows.

Letting $\lfloor . \rfloor$ be the *floor* function, if $2\lfloor np/2 \rfloor < np$, then np is not an integer. In this case, let $\hat{Q}(p) = x_{\lfloor np \rfloor + 1}$. If np is an integer, let $\hat{Q}(p) = x_{np}$ (SAS 2025). As an illustration of how this estimator works, consider the sample {1, 2, 3, 4} taken from the ordinal random variable, X. Say that each of its four possible values are equally likely. The sample quantile, $\hat{Q}(0.2) = 1$ because $F(1) = 0.25 > 0.2$ – satisfying the above quantile function definition. And for the sample, {1, 2, 3, 4, 5} taken from the ordinal random variable, Y having five equally likely values, $\hat{Q}(0.7) = \hat{Q}(0.8) = 4$.

This quantile estimator is used to compute the sample median, $\hat{Q}(0.5)$ and the sample IQR, $\widehat{IQR} = \hat{Q}(0.75) - \hat{Q}(0.25)$ from the three sample *quartiles;* $\hat{Q}(0.25)$, $\hat{Q}(0.50)$, and $\hat{Q}(0.75)$. For example, say that a query result contains a set of names: {Ben, Jerry, Ralph, Linda, Mary}. Sorting the associated set of index values might yield: {1, 4, 9, 17, 23}. This data set's sample median and sample IQR are 9 and $17 - 4 = 13$, respectively. The third statistic used to summarize the values on a particular attribute in the i^{th} query result is the tally of these values, $n_i^{(m)}$. In this example, $n_i^{(m)} = 5$.

Because all variables in the MNN's input vector need to take values on the unit interval, the median and IQR are divided by n_{att}, and the size measure, $n_i^{(m)}$ by n_d before they are added to the MNN's training data set.

Unlike a nominally- or ordinally-valued attribute, the values of a continuously-valued attribute such as the monetary size of a wire transfer, are used directly to summarize the query result rather than their associated index values. But similar to a nominally- or ordinally-valued attribute, the three statistics used to summarize a continuously-valued attribute in the i^{th} query result are the sample median divided by att_{max}, the sample IQR divided by att_{max}, and $n_i^{(m)}$ divided by n_d where att_{max} is the maximum value of the attribute in the database.

!!! Read to here !!!

2.5.5 Simulating query results

A JAVA program has been written by the author to simulate attribute data at the level of an ordered index. When $n_j^{(m)} > 1$, let s_i be the random interval between sampled index values where, for member j,

$$s_i \sim \text{Discrete-Uniform}\left(1,\ n_j^{(max)}\right). \tag{1}$$

The value of $n_j^{(max)}$ controls the disperson of the simulated index values and takes on one of the values in the set $\{1, \ldots,\ \lfloor n_d/(n_j^{(m)} - 1)\rfloor\}$. The chosen value for $n_j^{(max)}$ also indirectly affects the median of the sampled index values. For instance, if $n_d = 400$ and $n_j^{(m)} = 51$, then $n_j^{(max)}$ could be one of the integers one through eight. A simulated query result on this attribute is $\{x_1,\ \ldots,\ x_{n_j^{(m)}}\}$ where $x_1 = s_1$, and $x_i = x_{i-1} + s_i$, $i = 2, \ldots,\ n_j^{(m)}$.

When $n_d = 400$ and $n_j^{(m)} = 50$, a query result generated by member j might be characterized by an $n_j^{(max)}$ value of three. At some point in the future, however, this same member might, through bribery, extract a different query result on the same attribute. Such an insider attack could be simulated by setting $n_j^{(max)}$ to the value seven.

This simulation algorithm is new.

2.5.6 Example

Consider a confederation consisting of two members. Say that each member has their own, unique set of Structured Query Language (SQL) `where` conditions when submitting queries for the values on two attributes: player-name and associated vehicle registration number. Finally, say that there are $n_d = 300$ unique values on each of these attributes. Member 1's

queries result in $n_1^{(m)} = 5$ entities, and member 2's queries result in $n_2^{(m)} = 20$ entities. This behavior is simulated by generating a data set consisting of a size-40 set of query results on member 1 and a size-40 set of query results on member 2. These simulated sets of query results are generated with $n_1^{(max)}$ set to two, and $n_2^{(max)}$ set to 15.

Using one hidden node for each member, six input variables, and 18 parameters, the ITD fitted this data set in 7,367 function evaluations. At a randomly-generated starting point, the objective function's value was 1.0014, and 2.54E-14 at convergence.

Then, one day, member 2 queries the database for these same two attributes but now restricts the query to those players who have bank accounts. Players in this new query result will be somewhat different than those that are usually returned to this member. This behavior is simulated with member 2's new query result given in Figure 1. The ITD evaluated this new query result from member 2 and declared member 2 to be an insider threat.

Attribute 1	Attribute 2
2	4
4	10
7	12
11	22
18	23

Figure 1: Member 2's new query result in the ITD example.

2.5.7 Integrating insider threat detection into the FWCIDMS

Because the federated database of Haas (2023) uses PowerShell™ scripts to coordinate its various operations, the inclusion of this article's ITD can be incorporated within a computationally-efficient language (such as JAVA) that runs outside of the relational database software package. Specifics of how this integration is accomplished follow.

The logistics node is extended in the FWCIDMS to automatically collect a copy of each query result that is generated from every query issued by every member. Once a size-40 set of query results on member j is collected, the ITD begins to automatically check each new query result from every query issued by that member. Only those query results found to be non-threatening are added to member j's set of query results. If, as a result of one of these checks, the ITD declares member j to be a threat, the logistics node automatically sets member j's GLAD-defined global and local database access privileges to *none* and

simultaneously, sends a message to every other member stating that the ITD has declared member j to be a threat. Because all of these other members would then be aware of the threat, they would need to vote on whether member j should be separated from the confederation or not.

3 Identifying the most destructive traffickers

The simulator consists of (a) submodels of the decision making of several groups, and (b) a submodel of the ecosystem affected by these groups. Group submodels in the simulator lack a spatial location input node and hence do not indicate in their decision output where their decision to poach was executed. Here, for a particular group, such a spatial location is estimated by finding the temporally closest observed region that experienced a previous poaching event by that group. This procedure for estimating the region where a poaching action occurred is also used to spatially locate group-generated poaching actions that are predicted by the model to occur in the future.

Before being used to support a wildlife trafficking investigation, the simulator is statistically fitted via *consistency analysis* (CA) (Haas 2024a) to a *political-ecological* data set. This data set is composed of (a) an *actions history* data set collected via a STAR compliant protocol (Haas 2024b), and (b) an ecological data set. Then, this fitted simulator is run forward from the present time to a *planning horizon date* and the extinction risk at that time point is computed for each region. Using the formula for extinction risk given in Haas and Ferreira (2016), a region's local extinction risk depends in-part on its poaching rate through time, habitat availability through time, and prey availability through time.

After entering this region-risk information into their FWCIDMS, members issue queries to find players associated with regions having high local extinction risks and who are also enjoying high social network influence as expressed by their *eigenvector centrality*. This social network analysis measure is computed within the WCIT's social network model module. See Haas and Ferreira (2015) for a review of social network theory and associated measures as applied to the analysis of criminal intelligence.

The confederation then assigns the most influential of these players to their Detain list. Next, based on social network computations, the confederation assigns to their Surveil list, *Rising Stars* (players who are predicted to move into WTS leadership roles), and a

puppet master (an influential player attempting to hide their presence from law enforcement). Any pending trafficking actions detected by the confederation's intelligence-gathering are entered into their Interdict list. Finally, the confederation shares these three lists with law enforcement (governmental wildlife crime control agencies and international organizations pursuing prosecutions of wildlife traffickers).

In addition to the Detain, Surveil, and Interdict lists, this *actionable intelligence report* contains a *network resiliency* index for the WTS (a measure of how fast the syndicate's functionality can recover from a series of player arrests).

3.1 Estimating the syndicate's Rising Stars and resiliency

The social network model module of the WCIT assumes that the confederation gathers evidence on the WTS at three different time points. Intelligence gathered at the first time point is used to find out the size, connectivity, and assets of the current, undisturbed WTS. Next, the confederation quietly watches the network for several weeks and at the end of that period, observes its size and connectivity again. Then, the confederation recommends to law enforcement those WTS players to detain and surveil along with those near-future trafficking actions to interdict. Finally, some weeks after these arrests, 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.

Let $EC(p,t)$ be player p's eigenvector centrality at time t. Player p is a Rising Star if (a) $EC(p,t)$ is larger than the median eigenvector centrality of all players in the WTS network at time t; and (b) $EC(p,t_2) > EC(p,t_1)$.

Let $CI(t)$ be a measure of a social network's *connectedness* at time t. Connectedness is one way to measure a social network's *functionality*. Let *NRI* be a measure of a social network's resiliency defined to be proportional to how quickly a social network recovers 90% of its functionality after removal of some of its players.

One quantitative definition of $CI(t)$ is the largest eigenvalue of the social network's *link weight matrix*. And hence, one way to define *NRI* is to set it equal to $1/(t_3 - t_2)$ when $CI(t_3) = 0.9CI(t_2)$. This definition is operationalized by setting *NRI* to $CI(t_3)/((t_3 - t_2)0.9CI(t_2))$ when $CI(t_3) < 0.9CI(t_2)$ and declaring it to be at least $1/(t_3 - t_2)$, otherwise.

These two social network measures and the three-time-point strategy for attacking a

WTS are all new.

3.2 The Detain list's arrest sequence computation

Arrest-priority is assigned to those players who both reside in regions of predicted high local extinction risk and who have high eigenvector centrality. This prioritization is implemented by performing a a two-level sort of all players into an *arrest sequence* list. Sort level 1 is a descending sort of all players by the local extinction risk of the region of their residence. The second level is a descending sort on their eigenvector centrality at t_1. The Detain list is this arrest sequence list.

Because all players the confederation's database are included in this list, ecosystem damage is always the first priority when law enforcement arrests the first n players from this list no matter what n is. Depending on the political situation, law enforcement may have enough resources to arrest a large number of players.

In summary, the above arrest sequence list is produced by coupling a statistically fitted political-ecological model that hosts a preselected species to a social network model of the WTS that is harvesting that species. This coupling is new.

3.2.1 Discussion

Three points concerning this integration of political-ecological modelling and criminal intelligence need to be emphasized.

1. The fundamental challenge in biodiversity conservation is not the reduction of poaching but rather, the avoidance of local extinction events. This is why regions are prioritised by their local extinction risks rather than by their poaching rates.

2. These per-region extinction risks are generated by the simulator rather than by analysis of the confederation's associated social network model of those players contained in the confederation's FWCIDMS. And further, a political-ecological model is required in addition to a political-ecological data set in order to compute extinction risks at a future time point.

3. Criminal intelligence analysts may not be trained in ecology or in wildlife management and hence, need a single, quantitative measure of ecological damage that they can

incorporate into their criminal investigations. The ecologically sound, local extinction risk of a preselected species is one such measure.

4 Conserving the Cheetah

Many private, for-profit firms possess expertise in pursuing financial fraud investigations. Indeed, most insurance companies have an in-house *special investigation unit* (SIU) whose sole purpose is to investigate insurance fraud. Staff within such units include criminal intelligence analysts experienced in conducting criminal investigations that include the detection of financial irregularities from online sources. Such a firm would be in a position to assign one of their existing fraud investigation units to wildlife trafficking investigations. Call this wildlife trafficking investigations effort, the firm's *biodiversity project*.

A firm could fund this project with revenue from a *biodiversity premium* that they would charge in addition to the regular price of one of their products or services. Such a product or service is called a *biodiversity offering* (Haas 2022). The firm would market their biodiversity offering to customers who are concerned about biodiversity loss. The Intel kit of Haas (2025c) provides guidance, an example concerning the poaching of Bengal tigers (*Panthera tigris tigris*), and software to support a firm's efforts to develop such a business venture.

The following Sections describe how a wildlife trafficking investigations project could help conserve the East African cheetah.

4.1 The biodiversity offering and biodiversity project

Say that a hypothetical insurance firm has chosen one of their auto insurance policies for their biodiversity offering. Using revenue from the offering's biodiversity premium, this firm decides to focus on combatting cheetah trafficking where these animals are most populous: East Africa. The cheetah is listed as Vulnerable on the IUCN Red list and as Endangered by the Namibian government (Milloway 2025).

One form of such trafficking involves seizing live cheetah cubs in their den while their mother is away hunting. The few cubs who survive transport, are sold to private parties who desire an exotic pet (Tricorache et al. 2021). Countries where these seizures occur include

Kenya, Tanzania, and Uganda (Tricorache and Stiles 2021). Many of these transactions are arranged using social media platforms (Moneron and Nelwamondo 2024). In addition to these losses, local farmers shoot adult cheetahs to protect their livestock.

The firm reaches this decision in-part because much of the trafficking in cheetah is international wherein shipments originating in East Africa have final delivery locations in the Middle East and in the United States. Such international trafficking gives the firm's SIU opportunities to gather intelligence from many sources on shipments and the criminals managing those shipments. These sources include the internet and mobile phone networks.

The project consists of ongoing investigations of cheetah poaching events, cheetah poachers, cheetah cub shipments, cheetah body parts shipments, and the traffickers who (1) buy cheetahs and their body parts from poachers, (2) arrange transport of the ensuing shipments, and (3) arrange final retail sales of such shipments to consumers. Intelligence gathered in the course of these investigations is used to create a set of recommended law enforcement actions that is shared with the Kenya Wildlife Service (KWS) and the Tanzania Wildlife Management Authority (TAWA). These actions are conveyed in the Detain, Surveil, and Interdict lists as described above.

The project is implemented by leveraging current capabilities of the insurance firm's SIU. Specifically,

1. The firm assigns four SIU investigators part-time to the project. These investigators each bill one-third of their time to this project.

2. The firm joins a confederation of criminal intelligence analysts. This confederation maintains an FWCIDMS in order to allow members to share with each other, intelligence on traffickers and cheetah shipments. Further, this firm volunteers to maintain the logistics node of the confederation's FWCIDMS.

3. The firm purchases a secure hardware/software package to run this logistics node.

4. Finally, the firm hires and deploys a four-person team to Narobi, Kenya. This team consists of two criminal intelligence analysts, an office manager, and an information technology specialist. This team gathers evidence that can only be acquired by intelligence-gathering methods that are deployed on the ground in East Africa. These two analysts feed such intelligence to the confederation's FWCIDMS.

4.2 Monitoring program and cheetah abundance estimation

The confederation needs to statistically fit their cheetah-hosting political-ecological model to both an actions history data set and an ecological data set. Here, this ecological data set consists of real-time sightings of East African cheetah. This sightings data is streamed to the confederation's FWCIDMS.

Acquisition of sightings data in real-time requires the cooperation of East African conservation agencies. This cooperation is won through the services of the firm's *liaison consultant*. See Haas (2022) for a discussion of why this consultant is critical to the success of any in-country biodiversity project. And see Liaison (2025) for a step-by-step example of setting up a liaison office in a country that hosts a preselected species.

Once this sightings data is acquired, the work of Mallick (2023) can be followed as an example of using a *capture-recapture* statistical estimator to estimate the abundance of a terrestrial predator. A continuous-time approach to this estimation challenge is taken in Ferreira et al. (2020). A SAS code for such a computation with an accompanying example data set is available at Haas (2025c).

4.3 Cheetah-hosting political-ecological system simulator

The agent/individual-based model of the cheetah-hosting political-ecological system consists of the following submodels:

1. Kenya pastoralists, and Tanzania pastoralists
2. Kenya rural residents, and Tanzania rural residents
3. KWS and TAWA
4. The presidential office of Kenya, and the presidential office of Tanzania
5. A conservation-focused *nongovernmental organization* (NGO) operating in both of these two countries
6. A spatio-temporal, individual-based submodel of cheetah abundance.

See Haas (2025b) for the architecture, causal flow, and decision making mechanisim of the above group submodels. The cheetah abundance submodel is spatio-temporal because it computes an estimate of cheetah abundance for each politically-defined region in Kenya and Tanzania at each week over a specified interval of years.

4.4 Data sets

4.4.1 Actions history

A total of 1272 actions from 2009 through 2025 have been collected via the STAR compliant protocol developed by Haas (2024b). This actions history data set is summarized in Table 2. In particular, this data contains cheetah poaching actions that have occurred within specific regions.

Stories file name	Year(s)	Number of stories
ef9-13.txt	2009-2013	4178
ef13-14.txt	2013-2014	1655
ef14-15.txt	2014-2015	2443
ef15-16.txt	2015-2016	9293
ef16-19.txt	2016-2019	10910
ef19.txt	2019	9806
ef19-21.txt	2019-2021	8542
ef20211231.txt	2021	11623
ef20221231.txt	2022	30017
ef20230221.txt	2023	3016
ef20230529.txt	2023	2821
ef20231008.txt	2023	4605
ef20240111.txt	2024	2881
ef20240327.txt	2024	3173
ef20240609.txt	2024	3044
ef20240827.txt	2024	3508
ef20241112.txt	2024	3466
ef20250212.txt	2025	2391
ef20250315.txt	2025	1393
ef20250516.txt	2025	380
ef20250715.txt	2025	2405
ef20250906.txt	2025	2658

Table 2: Summary of the actions history data set. Stories files cover the years 2009 through 2025. Action detection is performed with the `parse_stories` relation of the FWCIDMS.

4.4.2 Ecological data

Cheetah sightings data is typically collected by field ecologists running camera traps or observing cheetah spoor. Based on these data-collection methods, the authors of World Population Review (2025) report 938 cheetah in Tanzania and 715 in Kenya. To show how a region-based abundance data set might appear, the World Population Review (2025) report is used to motivate a hypothetical, region-level cheetah abundance data set contained in the input file, `cheetahpatches.dat` (Figure 2).

```
patch_# patchname patch_area_(km2) cheetah_abundance nm_adjacent adj_patches
nmranches 1
kenyatanzania  20
 1 K_Marsabit       66923.1  600  1  3
 2 K_Amboseli         392.1    0  2  4 11
 3 K_Samburu        20182.5  400  2  1 10
 4 K_Tsavo          13747.0    0  1  2
 5 K_Maasai_Mara     1510.0    0  2  4 11
 6 K_Laikipia        8696.1    0  1  3
 7 K_Nakuru          7509.5    0  2  5  6
 8 K_Western         7400.4    0  1 10
 9 K_Central        11449.1    0  1  3
10 K_Turkana        71597.8    0  1  8
11 K_Kajiado        21292.7    0  3  5  2  4
12 T_Mara           21760.0  300  2  5 14
13 T_Shinyanga      18901.0    0  1 18
14 T_Arusha         37576.0  200  6 2 4 12 15 18 20
15 T_Manyara        44522.0    0  2 14 20
16 T_Dar_es_Salaam   1393.0    0  1 17
17 T_Tanga          26667.0    0  1 16
18 T_Simiyu         25212.0    0  3 12 14 13
19 T_Mwanza          9467.0    0  3 12 18 13
20 T_Kilimanjaro    13250.0    0  4 14  4 17 15
```

Figure 2: The input file, `cheetahpatches.dat`. Assignments of per-region cheetah abundances for the year 2025 are hypothetical. This file also contains inter-region adjacency information.

This file's inter-region adjacency relationships are read from the maps at Wikipedia (2025a), Masai Mara Travel (2025), and Wikipedia (2025b). Adjacency information is necessary to model cheetah movements across region boundaries.

4.4.3 Hypothetical criminal intelligence gathered on the WTS

The file, `cheetah_wts.dat` (Figure 3) contains the connectivity between players in the East African WTS that trades in live cheetahs and cheetah body parts. In this file, some of the syndicate's players are located in regions with high cheetah abundance: Marsabit and Mara (Figure 2).

```
linksfiletype nmtimepts
5             3
time_point nmplayers nmlevels nmlinks
0.0        10        4        11
name level town region country nmvehicles vehicles
r1 4 town1 marsabit      kenya 0
m3 2 town4 tsavo         kenya 0
m4 2 town1 maasai_mara   kenya 0
r2 4 town1 mara          tanzania 0
t2 3 town3 arusha        tanzania 0
t1 3 town1 tsavo         kenya 1 lu7
h22 1 town1 arusha       tanzania 0
m1 2 town1 marsabit      kenya 0
m2 2 town1 laikipia      kenya 0
h12 1 town1 marsabit     kenya 0
player 1 player 2 type
h12 m2 call
m2 h22 call
m2 m1 shipment
h22 m1 shipment
t1 m1 transfer
t2 t1 call
t2 r2 call
t2 r1 call
t2 m3 call
t2 m4 call
m3 m4 call
time_point nmplayers nmlevels nmlinks
17.0       10        4        13
name level town region country nmvehicles vehicles
r1 4 town1 marsabit      kenya 0
m3 2 town4 tsavo         kenya 0
m4 2 town1 maasai_mara   kenya 0
r2 4 town1 mara          tanzania 0
t2 3 town3 arusha        tanzania 0
t1 3 town1 tsavo         kenya 1 lu7
h22 1 town1 arusha       tanzania 0
m1 2 town1 marsabit      kenya 0
m2 2 town1 laikipia      kenya 0
h12 1 town1 marsabit     kenya 0
player 1 player 2 type
h12 m2 call
m2 h22 call
m2 m1 shipment
h22 m1 shipment
t1 m1 transfer
t2 t1 call
t2 r2 call
t2 r1 call
t2 m3 call
t2 m4 call
m3 m4 call
m2 m3 call
m2 m4 call
```

```
time_point nmplayers nmlevels nmlinks
24.7       9         4         9
name level town region country nmvehicles vehicles
r1 4 town1 marsabit      kenya 0
m3 2 town4 tsavo         kenya 0
r2 4 town1 mara          tanzania 0
t2 3 town3 arusha        tanzania 0
t1 3 town1 tsavo         kenya 1 lu7
h22 1 town1 arusha       tanzania 0
m1 2 town1 marsabit      kenya 0
m2 2 town1 laikipia      kenya 0
h12 1 town1 marsabit     kenya 0
player 1 player 2 type
m2 h22 call
m2 m1 shipment
h22 m1 shipment
t1 m1 transfer
t2 t1 call
t2 r2 call
t2 r1 call
t2 m3 call
m2 m3 call
```

Figure 3: Criminal intelligence gathered by the confederation on the WTS operating in East Africa.

4.5 Results

4.5.1 Parameter estimation and local extinction risk predictions

The above actions history data set and the above ecological data set form a political-ecological data set. This data set is used to statistically estimate the parameters of the Kenya rural residents, and the Tanzania rural residents submodels via the *Consistency Analysis* (CA) statistical estimator of Haas (2024a).

Due to computing resource limitations, only data from 2021 to 2025 is used to fit the model. CA increased the value of its statistical goodness-of-fit measure by 23.3% (Haas 2025a). The fraction of observed actions matched by the fitted model is 0.509.

Next, this fitted model is run forward in time to the planning horizon year of 2030 in order to predict local cheetah extinction risks by region (Table 3).

Country	Region	Extinction Probability	Extinction Risk
Kenya	Maasai_mara	00.333	00.278
Kenya	Western	00.266	00.222
Tanzania	Dar_es_salaam	00.066	00.055
Tanzania	Tanga	00.066	00.055
Kenya	Laikipia	1.000	0.000
Kenya	Nakuru	1.000	0.000
Kenya	Samburu	1.000	0.000
Kenya	Central	1.000	0.000
Kenya	Turkana	1.000	0.000
Kenya	Kajiado	0.000	0.000
Tanzania	Mara	1.000	0.000
Tanzania	Shinyanga	1.000	0.000
Tanzania	Arusha	1.000	0.000
Tanzania	Manyara	1.000	0.000
Kenya	Amboseli	0.000	0.000
Kenya	Tsavo	0.000	0.000
Tanzania	Simiyu	1.000	0.000
Tanzania	Mwanza	1.000	0.000
Tanzania	Kilimanjaro	1.000	0.000
Kenya	Marsabit	1.000	0.000

Table 3: Predicted local cheetah extinction risks by region for the year 2030.

These region-risk results are entered into the confederation's social network model mod-

ule in order to produce the actionable intelligence report that the confederation will share with law enforcement. This analysis is described next.

4.5.2 Construction of the actionable intelligence report

Using a social network model of the players contained in their FWCIDMS, the confederation constructs their actionable intelligence report as shown in Figure 4. This report is generated by running the **id** *relations file*, `kentan.id` with the command

```
idalone kentan.id
```

at a Windows or Linux command prompt depending on where the WCIT has been installed.

```
----- Detain List (Based on Network at Time point 1) -----

   Simulator-SNA-generated Optimal Arrest Sequence:
 Arrest_Priority  Extinction_Risk Eigenvector_Centrality  Player_Name
1    0.278    0.361   m4
2    0.0    0.552   r1
3    0.0    0.361   m3
4    0.0    0.352   r2
5    0.0    0.300   t2
6    0.0    0.244   t1
7    0.0    0.228   m1
8    0.0    0.228   h22
9    0.0    0.216   m2
10    0.0   0.092   h12

---- Surveil List (Based on Network at Time point 2) ------
SNA-generated Successor Prediction(s):
   r2 will succeed m4.
   m1 will succeed r1

SNA-predicted Influential Player Attempting to Hide
(highest ratio of betweenness centrality-to-degree centrality) =
     t1

SNA-predicted Rising Stars (Based on Time points 1 and 2):
   r1 is a Rising Star
   m4 is a Rising Star
   r2 is a Rising Star
   t1 is a Rising Star

------------------- Interdict List --------------------
           To Be Completed

--- Network Resiliency Index (Recovery Time) ---
  (assumes arrests were made just after time point 2)
  Connectivity Index at latest time =    2.518
   Connectivity Index prior to arrests =    3.166
   Network Resiliency Index =   00.114 or about   8.713 weeks.
```

Figure 4: Final section of the actionable intelligence report built from an integration of simulator-computed local cheetah extinction risks, and a social network analysis of the trafficker intelligence contained in the FWCIDMS. This report also contains several social network analysis measures that support the report's Detain, Surveil, and Interdict lists. Identity and location information of the players referred to in these lists is shared with law enforcement.

Figures 5 and 6 show the effects on the WTS due to the arrest recommended in the Detain list. These Figures indicate that the removal of player `m4` (a middleman) reduces the network's connectivity and isolates player `h12`. The WTS is expected to recover from this damage in about 8.713 weeks.

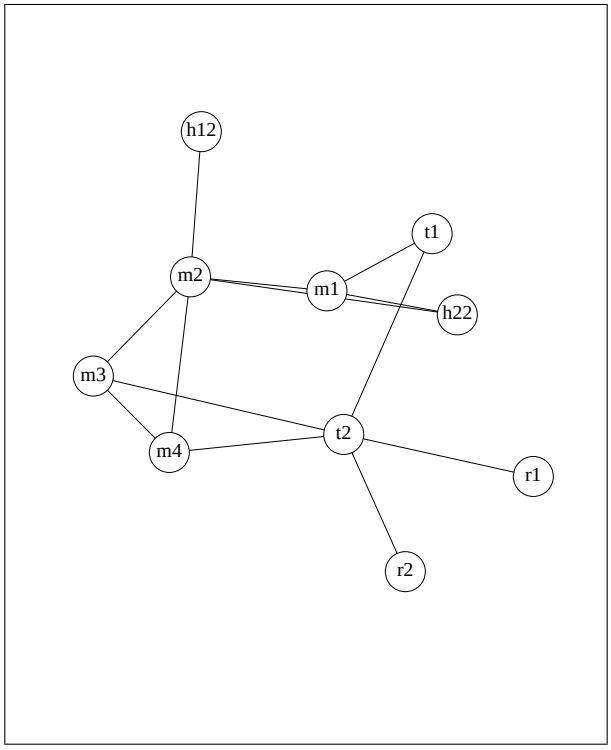

Figure 5: The syndicate's social network just before the arrest given in the Detain List is made.

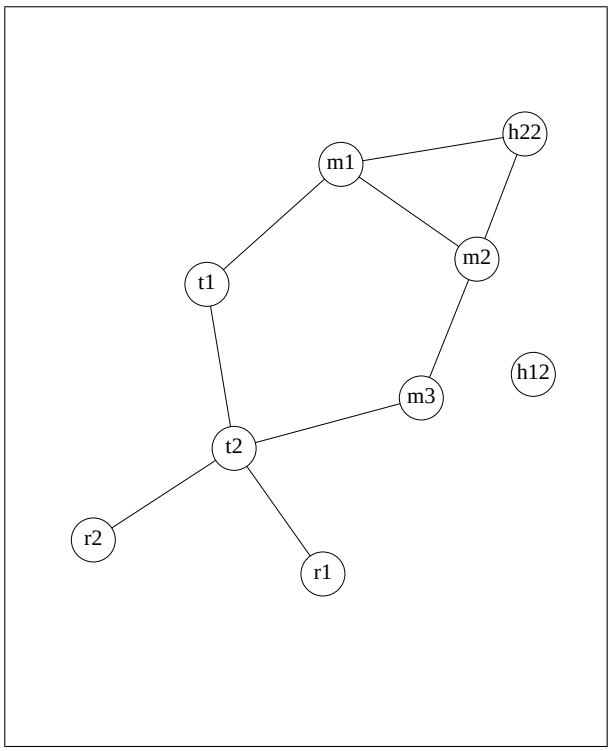

Figure 6: The syndicate's social network some weeks after the arrest of player `m4`.

5 Discussion

There is reason to believe that the most effective way to curb the illict trade in a particular species is to focus on interdicting those traffickers who reside in its home range and who are directly involved in its poaching and transport (Felbab-Brown 2018). If true, this strategy for fighting wildlife crime is congruent with one of the main points of this article: Anti-trafficking efforts should concentrate on species-hosting regions that are predicted to have high local extinction risks in the future.

5.1 Shortcomings

1. As discussed in Haas (2023), efforts to curb wildlife trafficking need to increase at least ten-fold in order to stem the rapid loss of global biodiversity (circa 2025). Intelligence-sharing agreements such as the confederation-approach developed in this article and in Haas (2023) are needed to help break the international syndicates that fuel this destruction of wildlife. But there are severe trust and financial roadblocks to overcome before such sharing can occur.

The ITD developed in this article is a start towards convincing the intelligence community that the sharing of wildlife trafficking intelligence need not compromise their security – but much more needs to be done before such analysts would actually be willing to share their hard-won, highly confidential criminal intelligence.

The biodiversity offering approach of Haas (2022) is also a start towards the funding of international wildlife trafficking investigations. But the needed increase in funding for increased wildlife crime investigations is so great that it is difficult to see how such funding increases could be accomplished within present funding mechanisms. Currently, such mechanisms are mostly based on private donations and the relatively low levels of taxpayer-support given to wildlife crime control agencies.

2. The per-region abundance data that is used herein to identify the most destructive traffickers is difficult to obtain for a variety of reasons. These reasons include lack of funding for monitoring; and difficulty in obtaining permission to take data on private land. An additional difficulty lies with those archiving such data and involves the fear that any web-based data repository will be hacked by traffickers seeking the locations of animals/plants to poach (Haas 2025a).

3. Within-database methods of detecting insider threats such as this article's ITD, are not useful at detecting those users who may become a threat in the near-future. To do this, it would be necessary to monitor each member's personal finances, contacts, and ideally, evidence of the member accepting bribes. Doing so would help prevent insider attacks from happening in the first place.

5.2 Future work

A more realistic example needs to be developed, analyzed, and displayed. This new example would contain actual per-region cheetah abundance estimates, actual per-region estimates of prey abundance, and a real-world trafficker intelligence data set. This latter data set may be challenging to obtain.

6 Conclusions

This article has described a working and freely available WCIT that can help a confederation of criminal intelligence analysts curb wildlife trafficking. This WCIT consists of three modules: An FWCIDMS, a political-ecological model of the system that hosts a preselected species, and a social network model of the WTS that is harvesting this preselected species. The latter two modules enable a confederation to focus their investigations onto those traffickers most responsible for the highest local extinction risks. This focus is enabled by integrating a model of a political-ecological system that hosts a preselected species with a social network model of the attacking WTS. Operationalizing this focus on high-extinction-risk traffickers within a wildlife trafficking investigation is new.

The most extensive actions history data set to-date (circa 2025) on cheetah trafficking has been collected by the author using a STAR compliant protocol (Haas 2024b). This data set has been used herein to show how this integration guides an investigation onto those traffickers most responsible for driving a preselected species towards extinction.

This article has also presented and tested a new, data-centric algorithm that protects the FWCIDMS module from insider attacks. This threat detection system is critical for convincing a diverse, multinational group of criminal intelligence analysts to voluntarily join a confederation that gathers, shares, and analyzes criminal intelligence to help curb wildlife trafficking.

To slow the rapid loss of biodiversity across the globe, it is crucial for wildlife trafficking investigations to be guided by credible models local species extinction risks. One way to provide such guidance has been presented in this article. Such political-ecological guidance of large-scale wildlife trafficking investigations may be the only way for such investigations to save those species who are on the brink of extinction.

References

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.

Castano, S., De Capitani di Vimercati, S., and Fugini, M. G. (1997), "Automated Derivation

of Global Authorizations for Database Federations," *Journal of Computer Security,* 5(4): 271-301, DOI: 10.3233/JCS-1997-5402.

Felbab-Brown, V. (2018), *To Counter Wildlife Trafficking, Local Enforcement, Not En-Route Interdiction, is Key, Brookings,* January 19. https://www.brookings.edu/articles/to-counter-wildlife-trafficking-local-enforcement-

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. DOI: 10.1111/aje.12728.

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-aft

Haas, T. C. (2025a), "Using Political-Ecological Models to Sustain Biodiversity," submitted to *Ecological Informatics*. Preprint available at www.profitablebiodiversity.com.

Haas, T. C. (2025b), "A Technology-Based Business Plan for Profitably Curbing Wildlife Trafficking," *Sustainability Technology* (SusTech 2025), Santa Ana, California, April 20-23. See page 50 of: https://ieee-sustech.org/wp-content/uploads/sites/261/2025/04/SusTech-2025-Program-Guide.pdf

Haas, T. C. (2025c) *Profitable biodiversity website.* https://profitablebiodiversity.com.

Haas, T. C. (2024a), "Models Vetted Against Prediction Error and Parameter Sensitivity Standards Can Credibly Evaluate Ecosystem Management Options," *Ecological Modelling*, 498, December, 11090 ("decreases" should be "increases" in the Graphical Abstract). DOI: 10.1016/j.ecolmodel.2024.110900.

Haas, T. C. (2024b). Protocol to Discover Machine-Readable Entities of the Ecosystem Management Actions Taxonomy. *STAR Protocols*, Cell Press, Elsevier, 5(2), 103125: 1-12. DOI: 10.1016/j.xpro.2024.103125.

Haas, T. C. (2023), "Adapting Cybersecurity Practice to Reduce Wildlife Cybercrime," *Journal of Cybersecurity*, 9(1): 1-20. DOI: 10.1093/cybsec/tyad004.

Haas, T. C. (2022), "Profitable Biodiversity," *Cogent Social Sciences*, 8(1): 1-24. DOI:

10.1080/23311886.2022.2116814.

Haas, T. C. (2021), "The First Political-Ecological Database and its Use in Episode Analysis," *Frontiers in Conservation Science, section: Planning and Decision-Making in Human-Wildlife Conflict and Coexistence*, 2:707088. DOI: 10.3389/fcosc.2021.707088.

Haas, T. (2020), "Developing Political-Ecological Theory: The Need for Many-Task Computing," *PLOS ONE*, November 24. DOI: 10.1371/journal.pone.0226861.

Haas, T. C. and Ferreira, S. M. (2016), "Conservation Risks: When Will Rhinos be Extinct?" *IEEE Transactions on Cybernetics*, 46(8): 1721-1734. Special issue on Risk Analysis in Big Data Era.
`http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7236914`.

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. DOI: 10.1186/s13388-015-0018-8.
`http://www.security-informatics.com/content/4/1/2`
`http://www.springer.com/-/4/0d7808225b2a4876986ead314e72ee99`

Koehler, G., Schmidt-Küntzel, A., Marker, L., and Hobson, K. A. (2023), "Delineating Origins of Cheetah Cubs in the Illegal Wildlife Trade: Improvements Based on the Use of Hair δ^{18}O Measurements," *Frontiers in Ecology and Evolution,* 11. DOI: 10.3389/fevo.2023.1058985.

Kul, G., Upadhyaya, S., and Hughes, A. (2020), "An Analysis of Complexity of Insider Attacks to Databases," *ACM Transactions on Management Information Systems,* 12(1): Article 4 (December). DOI: 10.1145/3391231.

Liaison (2025), *When To Set Up A Liaison Office in India 2024.*
`https://www.maiervidorno.com/blog/when-to-set-up-a-liaison-office-in-india/`

Mallick, J. K. (2023), "Conservation Status of Bengal Tiger Panthera tigris tigris in the Earth's Only Mangrove Tigerland: A Review of Efforts and Challenges," *Probe - Animal Science,* 5(1): 1-27. DOI: 10.18686/pas.v5i1.1777.
`https://probe.usp-pl.com/index.php/PAS/article/viewFile/1777/1688`

Marquis, Y. A. (2024), "From Theory to Practice: Implementing Effective Role-Based Access Control Strategies to Mitigate Insider Risks in Diverse Organizational Contexts,"

Journal of Engineering Research and Reports, 26(5): 138–154.
DOI: 10.9734/jerr/2024/v26i51141.

Masai Mara Travel (2025), *Map of Kenya*.
https://www.masaimara.travel/map-of-kenya.php

Mathew, S., Petropoulos, M., Ngo, H. Q., and 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,* 6307. Springer, Berlin, Heidelberg.
DOI: 10.1007/978-3-642-15512-3_20.

Milloway, O. (2025), *TWS 2024: Lead is 'Silently Poisoning' Captive Cheetahs, The Wildlife Society,* June 30. https://wildlife.org/tws-2024-lead-is-silently-poisoning-captive-cheeta

Moneron, S. and Nelwamondo, C. (2024), *Social Media Stimulating Trade in Cheetahs as Pets, Say New Data, Traffic,* March. https://www.traffic.org/publications/reports/online-live-cheetahs-trade-2024/.

Raywood, D. (2018), "Top Ten Cases of Insider Threat," *Infosecurity Magazine,* 25 December.
https://www.infosecurity-magazine.com/magazine-features/top-ten-insider-threat/

Redivo, E., Viroli, C., and Farcomeni, A. (2023), "Quantile-Distribution Functions and Their Use for Classification, with Application to Naïve Bayes Classifiers," *Statistics and Computing,* 33(55). DOI: 10.1007/s11222-023-10224-4.

SAS (2025), *PCTLDEF=3* (in) *Computing Quantiles, SAS/STAT 15.3 User's Guide.*
https://documentation.sas.com/doc/en/statug/15.3/statug_stdize_details03.htm

Setiono, R. and Hui L. K. (1995), "Use of a Quasi-Newton Method in a Feedforward Neural Network Construction Algorithm," *IEEE Transactions on Neural Networks,* 6(1): 273-277. DOI: 10.1109/72.363426.

Tricorache, P., Yashphe, S., and Marker, L. (2021), "Global Dataset for Seized and Non-Intercepted Illegal Cheetah Trade (Acinonyx jubatus) 2010–2019, *Data in Brief,* 35(106848).
DOI: 10.1016/j.dib.2021.106848.
https://www.sciencedirect.com/science/article/pii/S2352340921001323.

Tricorache, P. and Stiles, D. (2021), *Black Market Brief: Live Cheetahs*, *Global Initiative against Transnational Organized Crime*, September. https://globalinitiative.net/wp-content/uploads/2021/09/GITOC-ESAObs-Live-Cheetahs-Black-Market-Brief.pdf.

Wang, R., Li, C., Zhang, K., and Tu, B. (2025), "Zero-Trust Based Dynamic Access Control for Cloud Computing," *Cybersecurity*, 8(12). DOI: 10.1186/s42400-024-00320-x.

Wikipedia (2025a), *Kenya Counties*.
https://en.wikipedia.org/wiki/Counties_of_Kenya

Wikipedia (2025b), *Regions of Tanzania*.
https://en.wikipedia.org/wiki/Regions_of_Tanzania

World Population Review (2025), *Category: Environment*.
https://worldpopulationreview.com/country-rankings/cheetah-population-by-country