Adapting Cybersecurity Practice to Reduce Wildlife Cybercrime

Timothy C. Haas, Emeritus Associate Professor (Statistics)

Sheldon B. Lubar College of Business, University of Wisconsin-Milwaukee, haas@uwm.edu, *Industry Affiliate*, UCLA Department of Computer Science, and *Director*, Profitable Biodiversity; https://sites.uwm.edu/haas/; https://profitablebiodiversity.com

- Ph.D., Statistics, Colorado State University, 1989; Acting Assistant Professor, Department of Statistics, the University of Washington; Sabbaticals at the National Center for Atmospheric Research, Department of Statistics, Stanford.
- In collaboration with South African National Parks, developed a social network analysis of a rhino poaching syndicate, and a model of the political-ecological system that drives South Africans to poach rhinos.
- Work published in Journal of the American Statistical Association, Forest Science, Atmospheric Environment, Environmetrics, AI Applications, Stochastic Environmental Research and Risk Assessment, Security Informatics, IEEE Transactions on Cybernetics, Ecological Applications, PLoS One, Frontiers in Conservation Science, Journal of Cybersecurity, Wiley Research Monographs, Cogent Social Sciences, and Cell STAR Protocols.
- Grants from USDA Forest Service, US-EPA, WWF.

Research Projects

- Develop a business model wherein firms market profitable offerings that conserve biodiversity. Do this by tying the offering to a biodiversity project that focuses on conserving a specific species.
- Develop a web-based dashboard of data from the real-time monitoring of the project's at-risk ecosystem so that customers continue to purchase the *biodiversity offering*.
- Develop a peer-to-peer criminal intelligence database that can help bring wildlife traffickers to justice.

Table of Contents

- How to Sustain Biodiversity
- A Confederation of Wildlife Crime Investigators
- The Confederation's Databases
- Global Authorization Derivation (GLAD) Database Access Control
- Wildlife Trafficking Syndicate (WTS) Example

Biodiversity is Going Away

- The sixth mass extinction in the history of the planet is underway.
- Most large, wild mammals, many fish species, and many rare plants will be gone by 2060.
- Current conservation strategies are not working.

Sharks and Elephants

- The great white shark, a particular species of fish is endangered.
- And the African savanna elephant was added to the IUCN Red List in 2021.

And Cycads

For instance, the cycad plant, poached as a status symbol and investment, has been on this planet for about 280 million years. Dinosaurs didn't show up until 245 million years ago.

Curbing These Human-Driven Extinctions

- The wholesale killing of animals and plants needs to stop, and habitat destruction needs to be curtailed.
- Recently, wildlife crime has become the most destructive force driving species extinctions – surpassing habitat destruction for the first time.

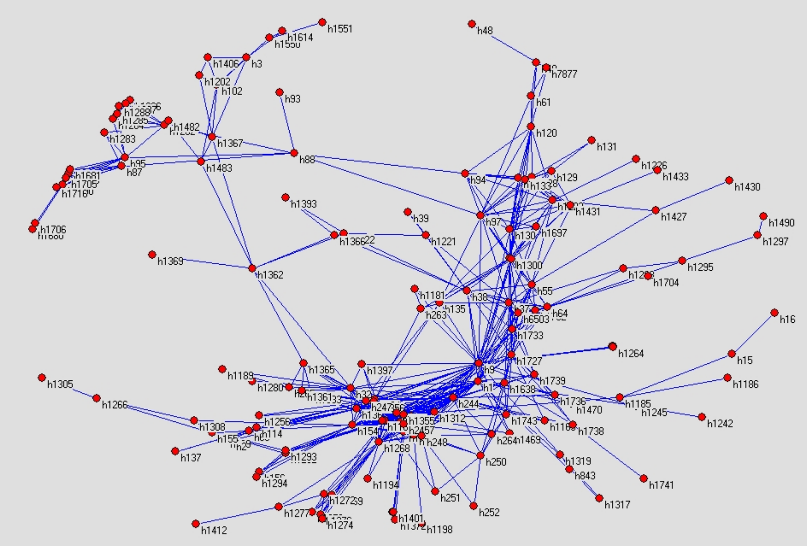
A Confederation and Associated Database

- Haas (2023) proposes a confederation of wildlife crime investigators that share a *trusted* criminal intelligence database.
- The confederation would analyze intelligence from cyber and non-cyber sources.
- Using these analyses, the confederation would deliver to law enforcement, recommendations for detaining, surveilling, and interdicting certain traffickers.

Confederation Actions

- The confederation would do this in two steps:
- **Step 1:** Compute an *actionable intelligence report*.
- **Step 2:** From this report, build the Detain, Surveil, and Interdict lists. Compute the syndicate's recovery time after those on the Detain list have been arrested.

December 2014 South African Rhino WTS



The 2014 Actionable Intelligence Report

```
---- 1. Centrality Measures ----
Player    Eigenvector                       Predicted Group
  h240         0.162                          middlemen
    h9         0.158                          middlemen
Player    Degree
    h9        75.000                          middlemen
  h240        61.000                          middlemen
Player    Betweenness
    h9     37516.993                          middlemen
   h97     25403.954                          middlemen
Player    Gould-Fernandez Total Brokerage
    h9      1889.0                            middlemen
  h240       960.0                            middlemen

 ---- 2. Optimal Arrest Sequence: h240 and then h9

 ---- 3. Successor Prediction(s): h1727 will succeed h240.
                                  h134 will succeed h9.

 ---- 4. Influential Player Attempting to Hide ----
         (highest ratio of betweenness centrality to degree centrality): h3

 ---- 5. Rising Stars ----
   Need 2 or more time points to predict rising stars.

 ---- 6. Recovery Time -----
   Need 2 or more time points to compute network resiliency index.
```

Confederation Deliverables

1. *Detain list*: A list of those WTS members (players) that law enforcement should detain for maximal disruption effect.
2. *Surveil list*: A list of those players that should be placed under surveillance for purposes of gathering evidence and/or information on future activities of the WTS.
3. *Interdict list:* A list of predicted WTS actions along with where and when these actions will take place. These actions should be interdicted.
4. *Recovery time:* An estimate of how long the WTS will take to recover from the removal of those players in the Detain list. Use this information to plan detention, surveillance, and interdiction operations.

The Logistics Office has Minimal Activities

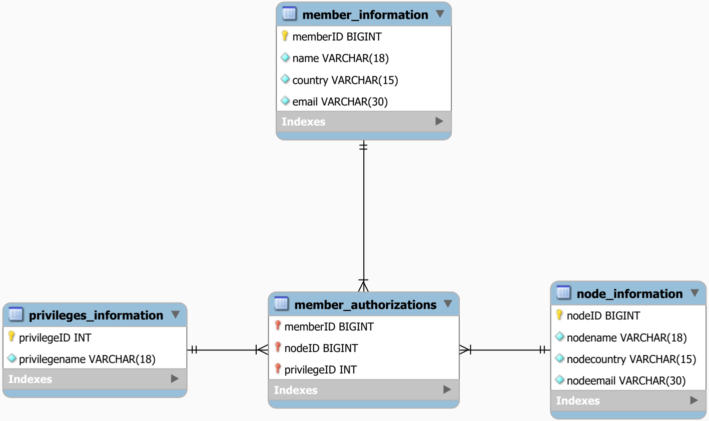
1. Support member-to-member communications.
2. Maintain the *logistics node* of the confederation's database and its access control tool.
3. Process membership applications and associated security auditor reports.
4. Prepare the confederation's budget and bill members for dues.

This is *rule-based management* among peers.

The Logistics Node Holds Only Administrative Data and Software

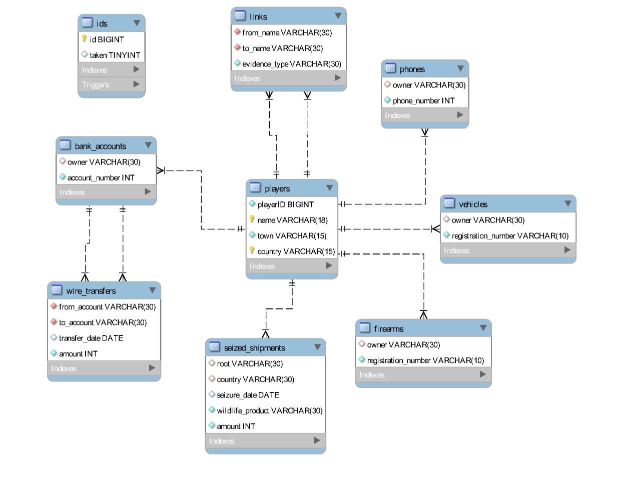
1. Member contact information; corruption index value; and information technology (IT) security index value.
2. Contact information for the corruption auditor and the IT security auditor.
3. The confederation's budget.
4. Ecosystem Management Tool (EMT) software and all database software.

The Logistics Node’s Database is Small



In this *entity relationship diagram*, a double bar into an entity indicates a source entity can map to only one entity whereas a trident indicates a source entity can map to many entities.

Confederation Database Tables



ids
- id BIGINT
- taken TINYINT
- Indexes
- Triggers

links
- from_name VARCHAR(30)
- to_name VARCHAR(30)
- evidence_type VARCHAR(30)
- Indexes

phones
- owner VARCHAR(30)
- phone_number INT
- Indexes

bank_accounts
- owner VARCHAR(30)
- account_number INT
- Indexes

players
- playerID BIGINT
- name VARCHAR(18)
- town VARCHAR(15)
- country VARCHAR(15)
- Indexes

vehicles
- owner VARCHAR(30)
- registration_number VARCHAR(10)
- Indexes

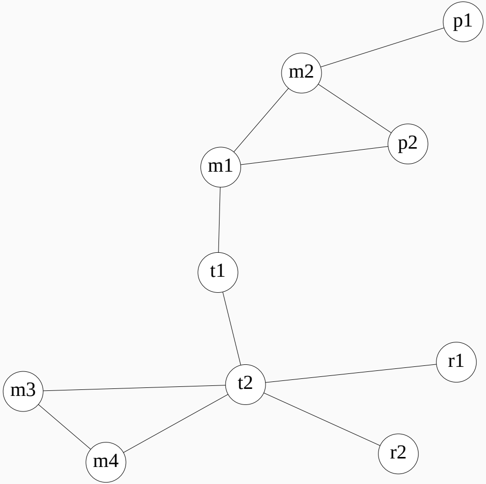
wire_transfers
- from_account VARCHAR(30)
- to_account VARCHAR(30)
- transfer_date DATE
- amount INT
- Indexes

seized_shipments
- root VARCHAR(30)
- country VARCHAR(30)
- seizure_date DATE
- wildlife_product VARCHAR(30)
- amount INT
- Indexes

firearms
- owner VARCHAR(30)
- registration_number VARCHAR(10)
- Indexes

Entity relationship diagram of the local database that runs on each node of the confederation's database.

A Hypothetical WTS



Poacher names: “p*;” middlemen: “m*;” traders: “t*;” and retailers: “r*.”

Player-to-Player Interactions Intelligence

Player 1	Player 2	Interaction type
p1	m2	call
m2	p2	call
m2	m1	shipment
p2	m1	shipment
t1	m1	transfer
t2	t1	call
t2	r2	call
t2	r1	call
t2	m3	call
t2	m4	call
m3	m4	call
t11	m1	call
t11	r1	transfer

Intelligence Gathered on Player Attributes

Internal identifier	Player name	Town	Country	Number of vehicles	Vehicles
h1	r1	A	Y	0	
h2	m3	B	Y	0	
h3	m4	A	Y	0	
h4	r2	A	Y	0	
h5	t2	B	Y	0	
h6	t1	A	Y	1	lu7
h7	p2	D	Z	0	
h8	m1	D	Z	0	
h9	m2	E	Z	0	
h10	p1	D	Z	0	
h11	t11	C	Z	1	lu7

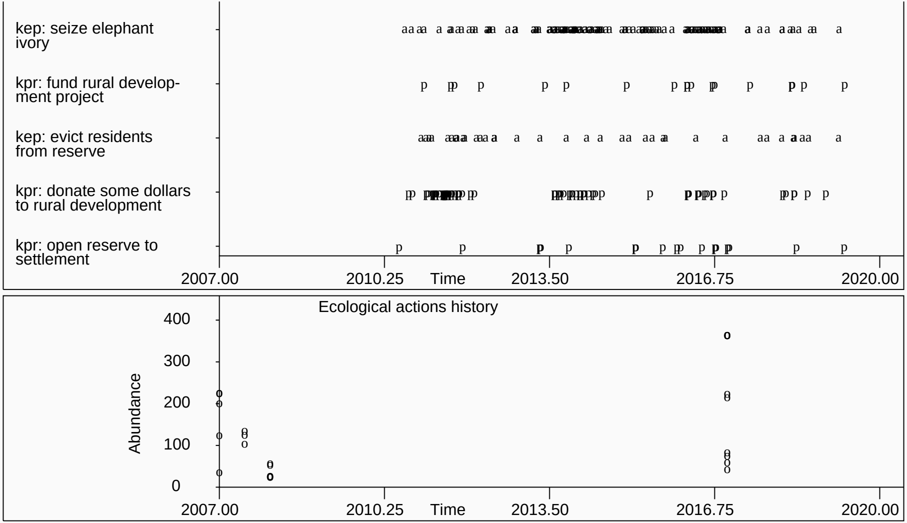
Who's Who

- Any person engaged in the physical, violent acquisition of animal parts for profit through the poaching (shooting, trapping, or poisoning) of live animals is referred to here as a *poacher*.
- As delineated in Haas (2023), poachers; middlemen that sponsor poaching raids; and those criminals who arrange shipments of poached animal parts are all *traffickers* who collectively, make up a WTS.

Simulating a Political-Ecological System

- The confederation's simulator simulates the decisions of all participants in the poached species' ecosystem. The abundance of this species is also modeled.
- All of these submodels interact with each other through time.

A Political-Ecological Data Set (Cheetah)



The Simulator's Submodels

- There are also agent-based submodels of decision making by several identified poachers; several identified middlemen involved in buying, transporting, and selling animal parts; consumers of these poached animal parts; and the wildlife crime control bureau.
- The simulator's ecosystem submodel is an individual-based, population dynamics model of the abundance of the species being poached.

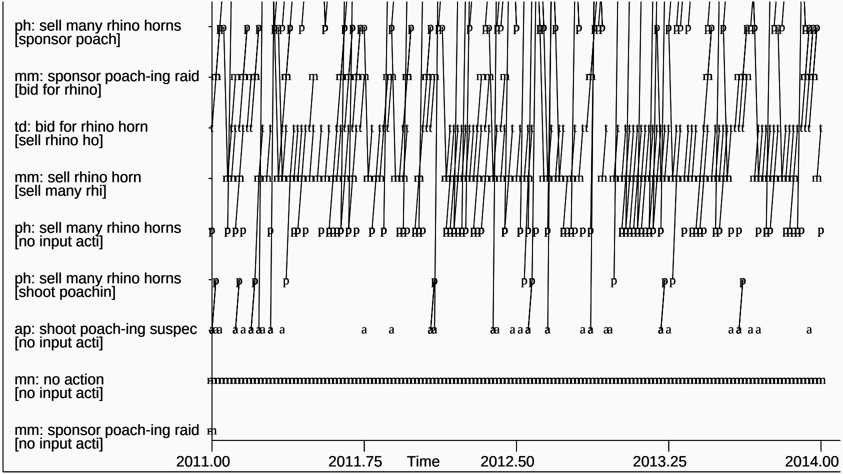
The Simulator Identifies the Most Destructive Traffickers

- The simulator is first, statistically fitted to a political-ecological data set.
- Then, this fitted simulator is then used to predict the poaching rate assuming a certain set of traffickers are active in the simulation.
- These predictions are used to assign traffickers to the confederation's Ecosystem Effects sublist.

Individual and Group Submodels

- The consumer submodel along with the wildlife crime control bureau submodel simulate group-level decisions.
- Individual-level submodels are built for each identified trafficker be they a poacher or a middleman.
- Individual submodels are linked to the associated nodes of the confederation's *social network model* of all traffickers in their database.

A Fitted Simulator's Actions History



mn indicates *no group*.

Actionable Intelligence Report 1

```
           ACTIONABLE INTELLIGENCE REPORT

---------- Social Network Analysis Metrics -------------
 Player  Eigenvector  Degree      Predicted
         Centrality   Centrality  Level
    t2        00.552       5.000     3      (trader)
    m4        00.361       2.000     2      (middleman)
    m3        00.361       2.000     2
    t1        00.352       2.000     3
    m1        00.300       3.000     2
    m2        00.244       3.000     2
    r2        00.228       1.000     4      (retailer)
    r1        00.228       1.000     4
    p2        00.216       2.000     1      (poacher)
    p1        00.092       1.000     1

           Betweenness Between/Degree
    t2          68.000       13.600    3
    t1          58.000       29.000    3
    m1          54.000       18.000    2
    m2          34.000       11.333    2
    m4          18.000        9.000    2
    p2          18.000        9.000    1
    m3          18.000        9.000    2
    r2          18.000       18.000    4
    p1          18.000       18.000    1
    r1          18.000       18.000    4
```

Report 2: Potential Information Brokers

```
           Gould-Fernandez
           total brokerage
    t2          9.0       3
    m1          2.0       2
    m2          2.0       2
    t1          1.0       3
    m4          0.0       2
    p2          0.0       1
    m3          0.0       2
    r2          0.0       4
    p1          0.0       1
    r1          0.0       4

 ------------------ Detain list ------------------
SNA sublist.
Optimal Arrest Sequence:
t2 is the first player to arrest and t1 is the second player to arrest.

Ecosystem Effects sublist.
players t1, p2, m1
```

The Ecosystem Effects sublist is found from simulator output.

Report 3: Surveil List and Communities

```
-------------------- Surveil list ----------------------
Successor Prediction(s):
r2 will succeed t2.
m1 will succeed t1

Influential Player Attempting to Hide (highest ratio of betweenness
centrality to degree centrality): t1

Rising Stars: Need 2 or more time points to predict rising stars.

Community Structure.
Number of communities: 2

 Player    Community
    r1         5
    m3         5
    m4         5
    r2         5
    t2         5
    t1         5
    p2         8
    m1         8
    m2         8
    p1         8
```

Report 4: WTS Actions to Interdict

```
----------------- Interdict list -------------------
January 2016: m3 will sell rhino horns in town B, country Y

------ Network Resiliency Index (Recovery time) --------
Current network's connectivity index value:   2.592
   Need 2 or more time points to compute network resiliency
   index.
```

The GLAD Access Control Tool

- This tool, developed by Castano et al. (1997), automates the task of deciding who may access what in a federated database and enforces all restrictions imposed by nodes for access to their local databases that, collectively, make up the confederation's database.
- The tool consists of the following three modules.

GLAD Access Control Tool Modules

1. *Local Security:* Specifies the local authorization policy of each node.
2. *Global Security:* Runs algorithms to combine all exported local authorizations into global ones.
3. *Dictionary:* Executes operations on nodes as per requests from (access-controlled) confederation members.

GLAD Access Control can be Conservative

The GLAD access control tool can be configured to implement a *strictly conservative* access authorization strategy that ensures global authorizations derived from exported local authorizations do not result in a member being given global access privileges that exceed the lowest level of privileges given to that member across all nodes.

Confederation Database Scripts

Script	Purpose
Local Security module	
1. create_node.sql	Create a database node.
2. *required_changes.sql	Change the privileges of one or more members as dictated by a single node.
Global Security module	
3. create_logistics.sql	Create the logistics node database.
4. update_glad.ps1	Manage an update of GLAD authorizations.
5. *compute_glad.sql	Compute GLAD authorizations.
6. *update_privileges.sql	Create an SQL script to update privileges.
7. global_privileges.sql	Update a node's GLAD authorizations.
8. *update_email.ps1	Send an email to a node directing it to run the attached global_privileges.sql.
Dictionary module	
9. fedquery.ps1	Run a query against the database.
10. example_query.sql	An example query.

*script is executed within update_glad.ps1.

Example of GLAD Access Control

Say that an investigator employed by the agency that is node 2 of the confederation has discovered that confederation member #51, John Doe has been bribed by a trafficker to post misinformation into the confederation's database.

Confederation Node 2 Forces an Access Control Update

```
************** User privileges granted at database creation *********
GRANT SELECT, INSERT, DELETE ON *.* TO ‘Jay Lee‘@‘%‘
GRANT SELECT, INSERT, DELETE ON *.* TO ‘Jeff Lee‘@‘%‘
GRANT SELECT, INSERT, DELETE ON *.* TO ‘John Doe‘@‘%‘

************** update_glad.ps1: Running required_changes.sql ********
delete from member_authorizations where memberID = 51 and nodeID = 2

insert into member_authorizations
   (memberID, nodeID, privilegeID) values (51, 2, 1)

************** update_glad.ps1: Running compute_glad.sql ************
set @nmnodes = (select count(nodeID) from node_information)

delete from member_authorizations where nodeID = 0
```

SQL Script to Update Access Authorizations

```
create temporary table n (
   memberID bigint unsigned not null default 0,
   privilegeID int unsigned not null default 0,
   nmgivenpriv int unsigned not null default 0,
   nodeID int unsigned not null default 0)

insert into n (memberID, privilegeID, nmgivenpriv)
   select memberID, privilegeID, count(*) as nmgivenpriv
   from member_authorizations
   group by memberID, privilegeID
   having nmgivenpriv = @nmnodes

delete from n where memberID = 0
update n set nodeID = 0
set foreign_key_checks=0
insert into member_authorizations (memberID, nodeID, privilegeID)
   select memberID, nodeID, privilegeID from n
```

Updated Database Access Authorizations

```
select * from member_authorizations

1    0   1
1    1   1
1    2   1
9    0   1
9    1   1
9    2   1
51   0   1
51   1   1
51   2   1
1    0   2
1    1   2
1    2   2
51   1   2
```

John Doe first has all privileges revoked on node 2; then privilege 1 on node 2 added. The result is that privilege 2 (insertion) on node 2 has been removed.

SQL Script Emailed to Every Database Node

```
************** update_glad.ps1: Running update_privileges.sql *******
************** global_privileges.sql ******************************
grant select  on *.* to ’Jay Lee’;
revoke all on *.* from ’Jay Lee’;

grant select  on *.* to ’Jeff Lee’;
revoke all on *.* from ’Jeff Lee’;

grant select  on *.* to ’John Doe’;
revoke all on *.* from ’John Doe’;
flush privileges;

grant select on *.* to ’John Doe’;
show grants for ’John Doe’;
GRANT SELECT ON *.* TO ‘John Doe‘@‘%‘;

grant select on *.* to ’Jeff Lee’;
show grants for ’Jeff Lee’;
GRANT SELECT ON *.* TO ‘Jeff Lee‘@‘%‘;

grant select on *.* to ’Jay Lee’;
show grants for ’Jay Lee’;
GRANT SELECT ON *.* TO ‘Jay Lee‘@‘%‘;
grant insert on *.* to ’Jay Lee’;
show grants for ’Jay Lee’;
GRANT SELECT, INSERT ON *.* TO ‘Jay Lee‘@‘%‘;
flush privileges;

************** update_glad.ps1: Running update_email.ps1 ************
(output not shown)
```

The Untrusted Member Attempts a Query

```
******** example_query.sql: run on node #2 *************
use node2;
insert into phones (owner, phone_number)
   values(’m3’, 123456789);

******** example_query.sql: output *********************
ERROR 1142 (42000) at line 8: INSERT command denied to user
’John Doe’@’localhost’ for table ’phones’
```

Conclusions

- International wildlife trafficking is destroying biodiversity. An international, peer-to-peer criminal intelligence database would help bring these traffickers to justice.
- The biggest challenge to building such a database is *trust*. This challenge can be overcome by the above-developed confederation organization and associated GLAD-accessed database.

Future Work

- Build an experimental confederation and associated criminal intelligence database. Acquire user impressions of its effectiveness and trust levels.
- Most governments and many NGOs have wildlife trafficking investigation units. Demonstrate this confederation organization and associated database to them.

The Proposal's Scripts and Codes are Available

- All SQL, Windows PowerShell, and DOS batch files can be downloaded from either Haas (2023: Supplement) or from `profitablebiodiversity.com`.
- And, all JAVA$^{\text{TM}}$ source code for the **id** software package can be downloaded from `profitablebiodiversity.com` (kit #3).