Proposal to ??:
Tools to Secure and Analyze Cybercrime Intelligence
DRAFT

Co-principal investigators:
Timothy C. Haas, Director, *Profitable Biodiversity*
& ??

1 Summary

Amount requested: $100,000
Grant Duration: 1 year
Number of supported students: 1

Advances will be made in the area of secure peer-to-peer cyber trafficking investigations, and location-masked images. These cyber trafficking tools can be used to investigate all types of cyber trafficking such as narcotics, firearms, humans, and wildlife.

2 Deliverables

2.1 Databases to support trafficking network investigations

1. Open software will be developed for the secure querying of a closed federated database of criminal intelligence on traffickers.

2. Methods will be developed for identifying key traffickers by their direct impact on trafficking pipelines rather than by their values on social network metrics alone.

3. A federated database query algorithm will be developed that is resistant to insider threats.

2.2 Preventing the misuse of ecological images

1. Tools will be developed that persistently acquire and format data from remote sensing resources for purposes of estimating the abundance of species that are under poaching pressure.

2. Security tools will be developed that removes geo-reference information from a sharable image so that it cannot be used to locate individual plants or animals to traffic. For instance, masking the geo-reference data in a digital species prevalence map renders it useless to poachers seeking to locate plants or animals to poach.

3 Rationale

3.1 Curbing wildlife trafficking

Wildlife trafficking is the fourth largest revenue generator for organized crime after firearms, narcotics, and humans (Haas 2023). Wildlife trafficking is driving many species to extinction and is overwhelming law enforcement efforts to stop it.

Wildlife traffickers often use the internet to commit their cybercrimes. Prosecuting such crimes is challenging. Indeed, one of the top five challenges in cybersecurity is to develop methods for pursuing cybercriminals and bringing them to justice through the acquisition of digital evidence that links specific individuals to specific illegal acts.

Database access control, also called information security (InfoSec), or data security is a chief component of cybersecurity. Haas (2023) proposes a distributed form of information security to keep a criminal intelligence database secure from unauthorized access and insider threats via a suite of peer-to-peer transactions. This approach, however, is dependent on lengthy polling activities between database members.

3.2 A criminal intelligence database of traffickers

Criminal syndicates kill and transport wildlife from source country to consumer country. For instance, in 2012, there were 10,000 rhinos in Kruger National Park (KNP), South Africa. Today there are about 3,000. Rhinos are shot for their horns that are then sold in Vietnam and China as traditional medicine.

Poachers and/or couriers, however, may be in contact with several different poaching rings. Further, players may have fled to another country to avoid prosecution. Shared criminal intelligence would help law enforcement prosecute these wildlife traffickers. This intelligence includes particular traffickers to arrest, particular wire transfers to block, and particular wildlife contraband shipments to interdict. Figure 1 is the entity-relationship diagram of a proposed federated criminal intelligence database (Haas 2023).

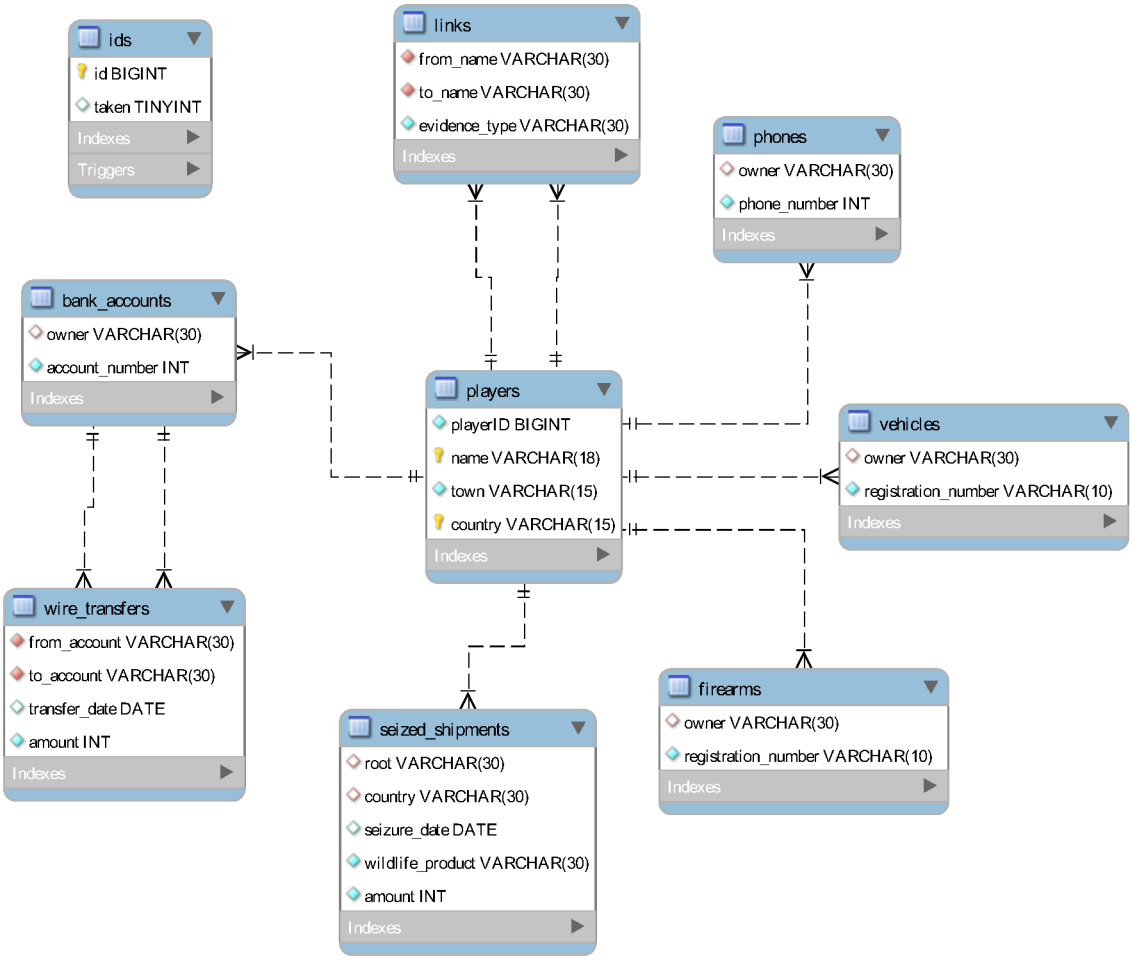

Figure 1: Entity-relationship diagram of a criminal intelligence database. Rectangles are entities. Rows within rectangles are attributes that take on values. A double bar symbol into an entity indicates a source entity can map to only one entity whereas a trident symbol indicates a source entity can map to many entities.

Actions may be local to a species-hosting country; concern interactions between consumption/donor countries and a species-hosting country; be taken by ecosystem managers; or be reactions by the ecosystem, itself.

3.2.1 Secure access to a criminal intelligence database

A criminal intelligence database is needed that focuses on wildlife traffickers. This database would include observations on those political-ecological actions that impact a species-hosting ecosystem. The database needs to be federated and secure against attacks by traffickers aiming to acquire information on criminal investigations and/or species locations. An access control system will be developed that can stop a member from setting all members' privileges to zero as a malicious effort to shutdown database. See Haas (2023) for an early attempt at such a system. The multidimensional trust-access control algorithm of Kim et al. (2022) will be a starting point to develop this access control system.

Such a database can become large. Hence, scalable query algorithms need to be developed. The work of Arnold et al. (2019) will be a starting point for this development.

3.3 Protecting ecological images

Figure 2 is a commercial satellite image of "Elephant Valley" at San Diego Zoo Safari Park. An algorithm developed in Haas (2018) correctly counts the thirteen elephants therein using only this image.

Figure 2: Elephant valley at Safari Park, San Diego Zoo.

Image-sharing procedures will be developed that secure such images from poachers trying to use them to locate plants or animals to poach. The image geo-reference encryption algorithm developed by Bhangale (2020) will be used as a starting point to develop this image security system.

3.4 Testing

All research outputs will be tested by using them to support rhino horn trafficker investigations.

4 Budget

4.1 Salary Support

Item	Date		Amount
1.	summer 2024	Professor ??: 1 month	$1,000.00
2.	2024	Student	$5,000.00
Total Direct Costs			$0
Indirect costs		(45% of Direct Costs)	$0
Total Salary Support			$0

4.2 Data

Satellite images.

Item	Date		Amount
1.	Summer 2024	Purchase of satellite images from ??	$1,000.00
Total Direct Costs			$0
Indirect costs (45% of Direct Costs)			$0
Total Software and Data			$0

4.3 Computing

Item	Date		Amount
1.	2024-2025	?? hours of computing time	$1,000.00
Total Direct Costs			$0
Indirect costs (45% of Direct Costs)			$0
Total Computing			$0

4.4 Travel

Item	Date	Description	Amount
1.	2024	Presentations at cybersecurity conferences	$10,000.00
Total Travel			$20,000.00

4.5 Total Requested

$??.

5 References

Arnold, J., Glavic, B., and Raicu, I. (2019), "A High-Performance Distributed Relational Database System for Scalable OLAP Processing," *IEEE International Parallel and Distributed Processing Symposium (IPDPS),* Rio de Janeiro, Brazil, pp. 738-748. DOI: 10.1109/IPDPS.2019.00083.

Bhangale, R. (2020), *Securing Image Metadata using Advanced Encryption Standard,* MSc Intership Cybersecurity, School of Computing, National College of Ireland. `https://norma.ncirl.ie/4149/`

Haas, T. C. (2018), "Automatic Acquisition and Sustainable Use of Political-Ecological Data," *Data Science Journal*, 17, p.17, DOI: 10.5334/dsj-2018-017

Haas, T. C. (2023), "Adapting Cybersecurity Practice to Reduce Wildlife Cybercrime," *Journal of Cybersecurity*, 9(1): 1-20. DOI: 10.1093/cybsec/tyad004. `https://academic.oup.com/cybersecurity/article/9/1/tyad004/7083342`

Kim, D., Alodadi, N., Chen, Z., Joshi, K. P., Crainiceanu, A., and Needham, D. (2022), "MATS: A Multi-aspect and Adaptive Trust-based Situation-aware Access Control Framework for Federated Data-as-a-Service Systems," *Proceedings of IEEE International Services Computing Conference (SCC) in IEEE World Congress on Services 2022*.