JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2023, 1–20
https://doi.org/10.1093/cybsec/tyad004
Research paper

Research paper

Adapting cybersecurity practice to reduce wildlife cybercrime

Timothy C. Haas *

Lubar College of Business, University of Wisconsin-Milwaukee, 3202 N. Maryland Ave., Wisconsin 53201, USA

*Correspondence author. Lubar College of Business, University of Wisconsin-Milwaukee, 3202 N. Maryland Ave., Milwaukee, WI 53201, USA. E-mail: haas@uwm.edu

Received 18 June 2022; revised 23 January 2023; accepted 27 February 2023

Abstract

Wildlife trafficking is driving many species to extinction and is overwhelming law enforcement efforts to stop it. At least a 2-fold increase in the number of traffickers who are put out of business is needed to help avoid these extinctions. A cybersecurity-based solution described in this article consists of a large international confederation of criminal investigators collecting intelligence on persons involved in wildlife trafficking, analyzing it, and then recommending to law enforcement (a) cybercriminals to detain, (b) cybercriminals to surveil, and (c) where and when to intercept cybercriminal-initiated wire transfers and shipments of wildlife products. Wildlife traffickers nowadays 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. The proposed confederation finds two lists of wildlife cybercriminals to remove. The first is found by computing centrality measures on the statistically estimated (reconstructed) current social network of wildlife cybercriminals to identify those criminals whose removal would, according to social network theory, maximally disrupt the syndicate's operations. This list contains criminals identified as kingpins, and/or information brokers. The second list consists of those *m* criminals whose removal results in the largest simulator-computed drop in poaching of the trafficked species over the next year. Database access control is a form of information security (InfoSec), or data security—a chief component of cybersecurity. Here, a distributed form of information security is developed for keeping a confederation's criminal intelligence database secure from unauthorized access and insider threats. This procedure uses only peer-to-peer transactions. The illegal trade in rhino horn is used to illustrate how this confederation would use criminal intelligence from several countries to first build a simulation of the political–ecological system that contains the trafficking operation, and then use this statistically fitted *simulator* to identify those traffickers to remove, wire transfers to block, and wildlife product shipments to seize. All software to implement this federated database and its access control procedure is freely available.

Key words: wildlife trafficking, wildlife cybercrime, organized crime, criminal intelligence database, social network analysis, InfoSec, data security, political–ecological system

Introduction

Biodiversity loss through wildlife product trafficking is happening at a cataclysmic rate that dwarfs current wildlife law enforcement efforts to arrest and prosecute wildlife crime suspects. For instance, during 2015–2020, INTERPOL aided law enforcement agencies in seizing many tons of wildlife being smuggled into various countries [1]. These law enforcement achievements are exemplary. During the last 50 years, however, the African elephant population declined by 75% [2]. And in just 10 years, the white rhinoceros (*Ceratotherium simum*) population declined by 24% due

to poaching [3], while the illegal trade in rhino horn continued unabated [4, 5].

Currently, the IUCN Red List contains 134 425 species of which 37 480 are at risk of extinction [2]. One study reports 958 of these 37 480 species are in danger due to trade [6]. A meta-analysis shows 506 species experiencing population declines exclusively due to trade [7]. About 6000 species, endangered or otherwise are being trafficked [8]. And, by accounting for the trade practice of substituting a similar species for a species that becomes too rare to harvest, Scheffers *et al.* [9] find that 11 702 vertebrate species face extinction from trade. The situation is also acute with regard to plants. Lavorgna and Sajeva [10] find that illegal trade in rare plants is driving many of them to extinction. Tittensor *et al.* [11] find that the volume of illegal wildlife trade is between 28 and 150% of legal wildlife trade. These figures are derived from seizure data at ports of entry. Because of the large number of shipping containers and the small number of customs inspectors, it is estimated that the volume of wildlife contained in seizures of shipments at ports of entry is only ∼10% of the total volume of wildlife traded illegally [12]. Between 30 and 90% of all live animals shipped illegally die in transit [13]. The effect on biodiversity from wildlife trafficking therefore, is most likely much higher than these sources can provide evidence for.

Habitat loss is often pointed to as the principal driver of biodiversity loss [14]. But a comprehensive study of biodiversity loss drivers finds no statistical difference between loss of habitat and *direct exploitation*, i.e. intentional harvesting of wildlife either legally or illegally [15]. While stricter regulations on legal exploitation such as the reduction of harvesting quotas might offer hope for some species, such regulations may negatively affect trafficked species as traffickers pursue profit opportunities that such regulation unintentionally provides. Thus, thousands of species will be lost unless wildlife trafficking is significantly reduced.

The US Fish and Wildlife Service has only 250 special agents pursuing wildlife crime investigations [16]. The US Drug Enforcement Administration on the other hand, has 2200 special agents [17]. And at ports of entry, the US Fish and wildlife Service is overwhelmed with the volume and frequency of wildlife shipments relative to their number of inspectors [18]. Because wildlife trafficking is the fourth most lucrative business of organized crime after firearms, narcotics, and humans [19], it is not unreasonable to assume that the number of wildlife criminals and number of wildlife crimes are about the same as the number of narcotics criminals and narcotics crimes, respectively. It would then follow that for the USA alone, at least a 10-fold increase in the amount of wildlife crime policing and interdiction is needed to help bring biodiversity losses down far enough to at least slow if not stop the mass extinction event that is currently underway [20].

Countries that are not as wealthy as the USA are experiencing even greater shortages of wildlife crime law enforcement. For instance, de Vries [21] concludes that Canada, having scarce law enforcement resources, needs to increase its cooperation with US law enforcement agencies in order to successfully prosecute international wildlife crimes. And specifically, such cooperation should be centered around the sharing of criminal intelligence. Jiao *et al.* [22] call for greater sharing of criminal intelligence between China and countries in Southeast Asia to curb wildlife crime. In many countries, corruption is a major driver of illegal wildlife trade and needs to be a part of all investigations of wildlife crimes [23].

Emphasis needs to be on the people involved in wildlife trafficking rather than on shipments of wildlife products—be they live plants, live animals, or parts thereof (e.g. logs, bones, bile, tusks, horns, claws, or scales). This is because the person who crated the illegal shipment of wildlife or wildlife products is usually untraceable [24, 25] and hence, intelligence on seized illicit shipments of wildlife or wildlife products is of limited use in an investigation of a particular trafficking suspect. Any project aimed at achieving such a massive increase in wildlife crime investigations and prosecutions will require at least an order of magnitude more law enforcement professionals who not only pursue wildlife crime cases but also share their criminal intelligence with each other. Any smaller effort will fail to stop these extinctions. It is unlikely, however, that a large number of internationally dispersed law enforcement professionals would agree to join a single, hierarchally managed policing organization—much less agree to surrender their own criminal intelligence to such an organization. Yet, in order to achieve a 10-fold increase in the number of traffickers put out of business, the combined intelligence from all of these investigators is needed to first, identify those traffickers causing the most damage, and then second, to bring enough evidence to bear on their prosecution so that they stop trafficking for a long time.

Wildlife traffickers nowadays often use the internet to conduct their crimes [26]. When wildlife traffickers use the internet to arrange transactions, make payments, or receive payments, they can be viewed as cybercriminals. Acquiring sufficient evidence on such a cybercriminal to successfully prosecute them and thereby shutdown their activities is difficult at best but essentially impossible without detailed data on their activities. Indeed, pursuing cybercriminals and bringing them to justice through the acquisition of digital evidence that links a specific individual to a specific illegal act was listed as one of the top five cybersecurity challenges for 2021 [27]. To successfully attack such an international problem, cybersecurity practice needs to adapt. For instance, many cybersecurity professionals work in a hierarchical organizational structure wherein policies are developed by senior management and implemented under the supervision of *security operations center* managers [28]. Reducing wildlife cybercrime, however, will need peer-to-peer management of a large number of independent wildlife trafficking investigators who work across many countries and who require that they retain control over who they trust [29, 30].

This article develops a new approach to conducting investigations into such *wildlife cybercrime* [31] that adapts cybersecurity practice in the areas of online, federated criminal intelligence databases; social network analysis of cybercriminals; and access management in peer-to-peer systems. These new practices take the form of an international confederation of wildlife crime investigation professionals who maintain a *federated database* [32] of wildlife crime intelligence (hereafter, simply *intelligence*) and use it to disrupt illegal activities that lead to biodiversity loss. Maintaining the security of this database and hence, the trust of a large number of investigators is addressed herein through a peer-to-peer database access control procedure. Database access control is a form of information security (InfoSec), or data security—a chief component of cybersecurity. InfoSec entails ensuring the confidentiality, integrity, and availability of data. Here, a distributed method is developed for keeping an intelligence database secure from unauthorized external access and from insider threats.

Traffickers often organize themselves into *syndicates*. One definition of a syndicate is "a loose organization of racketeers in control of organized crime" [33]. Disrupting the operations of a *wildlife trafficking syndicate* (WTS) can lead to reduced poaching of a trafficked species. This reduced rate of poaching in-turn, can temporarily cause that species' ratio of births to deaths to rise and hence buy time for it. Let a *player* be a person who is an active participant in a WTS. UN

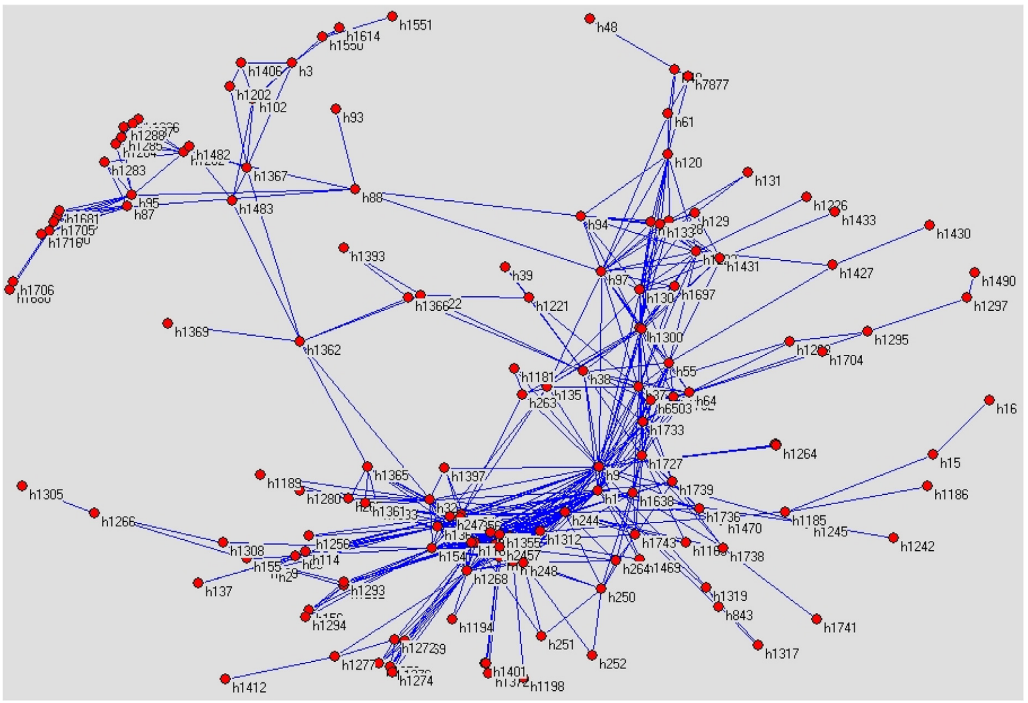

Figure 1: South African rhino poaching network as of December 2014. Players are poachers, couriers, and middlemen.

{[8], Chapter 8} identifies six different *levels* of players in a WTS: *poachers*, *runners*, *intermediaries*, *exporters*, *importers/wholesalers*, and *retail traders*. Here, these six levels are simplified by subsuming poachers and runners into *poachers*, subsuming *roots* (see below), *snakes* (see below), and intermediaries into *middlemen*, renaming exporters, *traders*, and subsuming importers/wholesalers and retail traders into *retailers*.

According to the Environmental Investigation Agency [34], a WTS operates as follows. *Poachers* harvest the wildlife product. Then, *runners* deliver the product to *middlemen* or *intermediaries* who in-turn, sell them to *roots* who have bribed port authority police to allow them to ship the product on to *retailers* in countries where wildlife products are consumed. Along the way, *traders* coordinate the various transactions with either payments in hard currency or, for larger transactions, with wire transfers between bank accounts. Wire transfers are also used by retailers to pay traders. *Snakes* come in two varieties: those who are paid by traders to tip-off poachers as to the whereabouts of targeted plants/animals (often, corrupted antipoaching rangers), and those government officials who are on the take with a WTS [35]. These latter individuals may work inside their government to impair law enforcement's efforts to disrupt the WTS's operations [23].

A WTS can be disrupted either by removing its *kingpins* and/or *information brokers*; seizing cash used by the syndicate to fund its operations and transact its business [34]; or seizing its shipments of wildlife products [36]. An information broker is a player who controls messaging between many different pairs of players [32]. For the specific disruption activity of targeted arrests of suspected traffickers, a larger reduction in poaching for the expenditure of the fewest resources can be had by arresting the syndicate's relatively few middlemen, traders, and retailers rather than the many on-the-ground poachers. This is because higher-level players typically control much of the syndicate's cash and coordinate many of its activities.

Example

Consider the poaching of rhinos for their horns. Horns are poached by chopping off a rhino's pair of horns after it has been shot with a hunting rifle. Arrest records and mobile phone transmission data are used to reconstruct the local component of the rhino horn trafficking syndicate operating around Kruger National Park (KNP) *circa* December 2014 (Fig. 1).

Centrality measures [37] from social network analysis (SNA) are computed on a *unimodal social network* [38] model of this WTS, called here, the *WTS network*. These measures help to identify players who are either kingpins or information brokers. Computation of each player's *eigenvector centrality* identifies players h9 and h240 as probable kingpins, and computation of each player's *betweenness centrality* identifies h9 and h97 as probable information brokers (Fig. 2). This *actionable intelligence report* [32] is given to law enforcement along with the following action recommendations. First, detain h240, then h9, and finally, h97. Second, serveil h1727 and h3.

Wildlife trafficking is transnational

An essential characteristic of a WTS is its transnational operation: Key players may reside in countries far removed from where wildlife is poached. For instance, in the above example, the list of players needs to be completed with data on players who operate outside of Africa. Local law enforcement is often unaware of who these individuals are—and for those they do know about, are usually unable to gather much intelligence on them nor muster enough evidence for successful extradition and/or prosecution proceedings.

Consider, for instance, the following scenario. Domestic law enforcement agency Z is unaware of relevant intelligence held by an agency located in another country—and only discovers this information by querying a database that contains all such intelligence. In particular, this agency learns that a trafficker, hiding in another country, is controlling a poaching and shipment operation in agency

```
          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.
```

Figure 2: An actionable intelligence report.

Z's country. This scenario suggests that domestic law enforcement agencies need to have much greater and more immediate access to intelligence held by law enforcement agencies in other countries.

Roadblocks

Below are the main reasons why wildlife trafficking is not being controlled at a sustainable level.

(1) Wildlife crime investigations often fail. Reasons for such failures include the following:
   a. current levels of financial support for international wildlife crime investigations are inadequate for the scale of the problem [39, 40];
   b. corrupt government officials are paid by traffickers to get shipments through customs and to shield them from criminal investigations [23, 40];
   c. law enforcement agencies do not trust each other enough to share their intelligence [41].

(2) Policies aimed at curbing wildlife trafficking do not account for the political situation that traffickers take advantage of. For instance, wildlife crime laws are not uniform across countries [8, 42, 43].

(3) Policies aimed at curbing wildlife trafficking are not tailored to the impact of anthropogenic actions on the population dynamics of a trafficked species. For instance, severe antipoaching laws are passed when in reality, habitat destruction is the main driver of a particular species' demise [44, 45].

A solution

The solution described in this article consists of a large international confederation of law enforcement professionals collecting intelligence on persons involved in wildlife trafficking, analyzing it, and then recommending to law enforcement (a) players to detain, (b) players to surveil, and (c) where and when to intercept WTS-initiated wire transfers and shipments of wildlife products. The confederation would create this actionable intelligence report by feeding its intelligence into first, a *federated*, *relational database*, and from there, into the Ecosystem Management Tool (EMT) software system of {Haas [46], Chapter 1}.

Confederation members would include individuals working in source countries, transport countries, and consumption countries. The confederation's ability to share intelligence across different countries would allow them to discover players who are attempting to hide their identity in some of the countries that they operate in. This ability in-turn, would allow the confederation to help law enforcement agencies to disrupt the WTS. The confederation would

accomplish this by performing a *deduplication* analysis on their intelligence.

The confederation would control access to their intelligence database with the Global Authorization Derivation (GLAD) database access control tool [47] (hereafter, simply the *GLAD access control tool*).

Elements of this solution are not new. For instance, nations routinely apply confiscation and sanctions to disrupt activities that are against their wishes. One example is the suite of sanctions levied by the USA against Iran [48]. Another is the routine practice by US law enforcement personnel of conducting in-country raids in order to seize drug contraband in Central America [49]. Another precedent is the Regional Information Sharing Systems (RISS) database [50]. This database, similar to the one proposed in this article, enables local, state, federal, and tribal law enforcement agencies in the USA to share intelligence with each other. The RISS confederation uses a regional structure to allow 9400 law enforcement agency members to share many types of intelligence across the US RISS membership is through a regional vetting process.

Materials and methods

Disrupting a WTS

A confederation to disrupt wildlife trafficking

An international group of wildlife crime investigators and analysts would self-select into a confederation. These confederation members (hereafter, simply *members*) would be otherwise employed at either law enforcement agencies, conservation-focused NGOs, private criminal investigation consultancies, or non-governmental, for-profit firms. These individuals would bring to the confederation a variety of crime-fighting specialties including detective skills, intelligence analysis, and forensic accounting [51, 52].

Say that this confederation is focused on the survival of a particular plant or animal. The confederation first models and then disrupts a transnational trafficking syndicate that is trading in this species. The confederation is aware that such syndicates usually offer a diverse product line including narcotics, humans, arms, wildlife, and wildlife products [53].

To support these modeling and disruption tasks, the confederation maintains a federated database of both open access data and secure intelligence. Open access data include news articles about poaching events; wildlife crime suspect arrests; trials involving defendants suspected of being players; or seizures of wildlife product shipments. The confederation builds a model of the political–ecological system that contains the WTS in the form of a *political–ecological simulator* (hereafter, *simulator*) {[46, 54], Chapter 1}. The parameters of this simulator are statistically fitted to observations queried from the confederation's database.

The confederation uses this fitted simulator to produce an actionable intelligence report. This report is distributed to law enforcement agencies and contains several recommended actions as follows.

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

How these components are found is described next.

Actionable intelligence 1: players to remove or serveil

The Detain list is composed of two sublists: one derived from social network theory, and one derived from ecosystem impacts. The SNA-derived sublist is found by computing centrality measures on the statistically estimated (reconstructed) current WTS network to identify a sublist of players whose removal would, according to social network theory, maximally disrupt the network's operations. This sublist typically contains players identified as kingpins, and/or information brokers.

This SNA-derived sublist, however, does not take into account the *direct* effect on the ecosystem due to the removal of certain players. These effects are, however, captured by the simulator because it contains dynamic mechanisms that govern both interactions of the WTS with other groups involved in the ecosystem that hosts the trafficked species—and interactions between all of these groups and the ecosystem. This makes the simulator a more complete model of the political–ecological system than the WTS network, alone. Also, theoretical work in social network theory [55] suggests that removing kingpins (those with high eigenvector centrality) may disrupt the syndicate's operations for only a short time, i.e. a WTS is *resilient* and therefore, will need to be repeatedly disrupted [32, 56]. Further, empirical evidence from real criminal networks suggests that because of how WTS operations are spread out among its players, such a network's operations are difficult to disrupt unless many players below the level of trader are removed [57, 58].

For these reasons, a second sublist is found of those m players whose removal results in the largest simulator-computed drop in poaching of the trafficked species over the next year. This sublist is found with the newly developed *optimal removal algorithm* (Appendix).

The Surveil list is found through computations on the reconstructed WTS network at the current time and as it existed 4 months previously. These computations yield (a) those players likely to succeed detained players; (b) those players who are influential but attempting to conceal themselves from law enforcement; (c) the network's *rising stars*; and (d) those players who make up tightly connected *communities* [59]. The productivity of a WTS is built from the bottom up by the functioning of these communities—each of whom is efficient due to their high internal connectivity.

Actionable intelligence 2: interdictions

When the simulator is run forward in time, a list is created of WTS actions that are indexed by date. This list holds predictions of future poaching events, future wire transfers, and future wildlife product shipments. These event predictions constitute the Interdict list.

Some of the money that flows through a WTS can be legally blocked. Many monetary (wire) transfers between players are SWIFT system requests that are usually routed through New York city banks [60]. The US Treasury's OFAC can force banks to block or reject SWIFT transactions of narcotics traffickers [60]. If certain players were added to the OFAC's list of Specially Designated Nationals (SDNs), examining the financial transaction records of these players would help to identify player-initiated wire transfers to block. Doing so would directly disrupt wildlife trafficking. Step one in this endeavor is to acquire evidence that a player initiating a wire transfer

is also a narcotics trafficker [53]. Thus, to use this blocking strategy, the confederation would need members who have access to narcotics trafficking intelligence.

Actionable intelligence 3: recovery time

Let the Recovery time, γ be the number of weeks after a disruption by law enforcement before the network regains 90% of its connectedness. Connectedness is measured by the *connectedness index*: The largest eigenvalue of the network's adjacency matrix [32]. At least one disruption operation by law enforcement needs to have been executed before γ can be estimated.

Confederation attractiveness, logistics, and selection protocol

Law enforcement agencies and individual law enforcement professionals would want to share their intelligence by joining a confederation for the following reasons. First, by doing so, they gain access to intelligence on suspects of interest to them that they might not be able to acquire otherwise. Such access would help increase their conviction rate for only a modest increase in their operating budget. Second, joining a confederation does not require that they give up control over who can access any intelligence that they collect through their own investigations.

The confederation's physical footprint is (a) a small *logistics office*; (b) some number of *nodes* located throughout the world that house local intelligence databases maintained by some of the confederation's members; and (c) some number of members who are not affiliated with any of the confederation's nodes. The logistics office maintains a database of members and their database access privileges as described in the section "Controlling database access," below.

Equitable and sustainable membership dues

The confederation maintains its logistics office through annual dues. Each year, this office prepares a budget whose total size is e. Say that there are n members of whom m have verified revenues (income) that are below an *income threshold* c. For instance, c could be set to twice the US Federal Poverty Level (FPL) for a one-person household. Then for 2023, c would be 27,180 USD [61]. Members whose income is $\geq c$ pay rc in dues, where r is the sliding scale dues rate for members whose income is $<c$. Members whose income is $<c$ pay rI_i in dues, where $I_i < c$, $i = 1, \ldots, m$ is member i's income. This latter formula is derived from the break even budget equation $e \geq (n-m)rc + \sum_{i=1}^{m} rI_i$, where $r = e/[(n-m)c + \sum_{i=1}^{m} I_i]$.

This hybrid flat-rate/sliding scale membership dues structure is one way to balance (a) the need to break even every year [63, 64]; (b) the desire to have most members pay an equal amount of dues to discourage unequal power relationships among members; and (c) the need to make membership feasible for individuals or agencies who have minimal financial resources but for whom confederation membership would be mutually beneficial.

Logistics office services

The only activities of the confederation's logistics office are:

(1) maintaining communications between all members;
(2) maintaining the *logistics node* of the confederation's database and the GLAD access control tool;
(3) processing membership applications and associated corruption auditor reports;
(4) preparing the annual budget and billing members for dues;
(5) inviting, cooperating with, and paying a licensed financial auditing firm to conduct the confederation's annual financial audit.

There are no other decisions that this office is authorized by members to perform. Hence, the confederation's management system is a form of *rule-based management* [62]. All other management decisions are made by individual members, all of whom are peers.

The logistics node holds a minimal amount of information consisting of the following:

(1) Member contact information.
(2) Each member's corruption index value and information technology (IT) security index value (see below).
(3) Contact information for the corruption auditor.
(4) EMT software including all database software.
(5) The confederation's budget and financial audit report.

Evaluating candidates for confederation membership

A concern members would have about a candidate is whether he/she would leak intelligence they receive from queries against the confederation's database with players or anyone else outside the confederation. Such leaking is not necessarily the result of a one-time bribe: There may be a snake on the candidate's staff who is paid by a WTS to provide them with information about ongoing investigations of the syndicate. But countries that have the most valuable intelligence may also have the most corrupt law enforcement agencies. And, these countries may also lack secure IT systems in their law enforcement agencies simply because they cannot afford more secure ones. Trust therefore, is seen as being two dimensional: a corruption dimension and an electronic data security dimension.

How can a confederation attract new members who have valuable intelligence without sacrificing intelligence security? One solution is as follows. To assess the trustworthiness of a candidate for admission into the confederation, the confederation hires a corruption auditor of their choice and pays them using the candidate's membership application fee. This auditor investigates the candidate and arrives at values for a *corruption index*, and an *IT security index*. The corruption index, CI is 0 if, over the previous 5 years, the auditor can find no reports of the candidate leaking intelligence, and no reports of bribery of the candidate's staff. CI equals 0.2 if there are two to three such reports, 0.5 if there are four to five, 0.8 if there are six to seven, and 1.0 if there are more than seven. This index is motivated by one proposed by Linhartová and Volejníková [65]. The IT security index is the pr metric of Yusuf *et al.* [66] defined to be the probability that a cyber attacker is able to penetrate the candidate's IT system and successfully download intelligence.

As one way to combine these two dimensions into a single trust metric, let a *trust index*, TR be defined as $1 - \max\{CI, pr\}$. Law enforcement professionals would join the confederation with the understanding that they will be separated from the confederation if their trust index falls below 0.4 and/or all of their database access authorizations are revoked.

The confederation's database

This database is used to maintain the simulator of the political–ecological system that the WTS is operating within, and a social network model of the WTS, itself. Observations on the simulator are called *action histories* {[46], Chapter 9} consisting of time-stamped actions taken by groups within the political–ecological system, and time-stamped values of ecosystem metrics such as the abundance of a trafficked species. Observations on the WTS are time- and player-

Table 1: GLAD access control tool modules and enacting scripts to maintain the security of a confederation's database, and allow queries against it.

SQL or PowerShell script	Purpose
	Local security module
create_node.sql	Create a database node.
*required_changes.sql	Change the privileges of one or more members as dictated by a single node.
	Global security module
create_logistics.sql	Create the logistics node database.
update_glad.ps1	Manage an update of GLAD authorizations.
*compute_glad.sql	Compute GLAD authorizations.
*update_privileges.sql	Create an SQL script to update privileges to GLAD authorizations.
global_privileges.sql	Update a node's privileges to GLAD authorizations. Generated by update_privileges.sql.
*update_email.ps1	Send an email to a node directing it to run the attached script, global_privileges.sql against their database in order to update the node's GLAD authorizations.
	Dictionary module
fedquery.ps1	Run a query against the federated database.
example_query.sql	An example query. Executed within fedquery.ps1

Files having extension ps1 are PowerShell scripts, and those with extension sql are SQL scripts. A "*" indicates a script that is executed within update_glad.ps1.

stamped. Connecting each observed WTS action to a player implements the model of a WTS as one social network and two networks of inanimate objects: the network of shipping ports, and the network of bank accounts. A shipping port is represented by the associated root, and a bank account is represented by the associated trader or retailer. Hence, the WTS network consists of only players, i.e. it is a strictly unimodal social network. Each vertex in the network is either an observed, named player or an archetypal stand-in for one.

A relational database models these two data streams through the components of *entities*, *relationships*, and *attributes*. An entity corresponds to something in the real world. An attribute is a measurable property of an entity. A particular case of an entity is an *entity instance* [67]. An entity instance has a *value* on each of its attributes.

Entities

The confederation's database consists of both open access data and secure intelligence acquired by members during the course of their investigation and surveillance operations. Extending the work of Haas and Ferreira [32], database entities are players, vehicles, firearms, bank accounts, wire transfers, and wildlife product shipments.

Attributes for these entities include

(1) personal information on all players including their names, addresses, and phone numbers;
(2) bank account numbers involved in a wire transfer between players; and
(3) locations of where wildlife product shipments were seized along with the product type and amount.

Federal agencies that are required by law to keep their data secret, such as the US Department of Defense or the US National Security Agency, would need to first declassify any data they wished to contribute to the confederation's database.

Database construction and visualization

The file create_logistics.sql (Table 1) creates the logistics node's database of confederation members along with their *database user privileges* (hereafter, *privileges*). This *structured query language* (SQL) script file is written in MySQL, a freely-available, multiplatform relational database management system (RDBMS) [68]. An SQL script file (hereafter, simply *SQL script*) is a text file. The SQL script create_node.sql (Table 1) creates an intelligence database on a single node and adds individual players plus player-to-player links to it. All of Table 1's SQL scripts can be run with few modifications within other RDBMSs including Microsoft's SQL Server™ [69].

The three PowerShell™ scripts in Table 1 help to automate database use and maintenance tasks. PowerShell is a modern, freely-available scripting language used to manage multi-user computing systems, and communicate between computers. It has been ported to many platforms including Windows, Mac, and Linux [70].

The *entity relationship diagram* of this federated database is drawn with MySQL Workbench [68] (Figs 3 and 4).

Data formats and database querying

A challenge with a federated database is that different nodes may use different data formats. This in-turn, can make it difficult to combine data from different nodes. As Hasselbring [71] discusses, *wrappers* can be used. These are local programs that re-format database variables (entities and attributes) into the format of each node. When a query is run against the database, table and attribute names are translated from a set of generic names into the names used by each node.

Wrappers are implemented as follows. First, the logistics node maintains a PowerShell script that contains (a) the URLs of all current nodes; and (b) the map between each generic name of a database table or attribute—and those names used by individual nodes, e.g. fedquery.ps1 (Table 1). Second, a member formats his/her query as an SQL script using generic names for table and attribute names. Then, the member submits this script on the logistics node by entering the following at a Windows, Mac OS, or Linux command prompt:

```
powershell ./fedquery.ps1 example_query.sql > query_result.txt,
```

where example_query.sql (Table 1) is one such query.

If the query contains SQL commands that are not globally authorized for that member, the script returns INSUFFICIENT AUTHORIZATION and the query fails. In this case, the member needs to either abandon the query or modify it so that it does not exceed his/her global authorizations. If the query is successful, the member receives a concatenated file of the results of the query applied against every node's database.

Because this access control tool is automatic, the database can be maintained and queries processed by a small staff of database support personnel employed across the confederation's nodes.

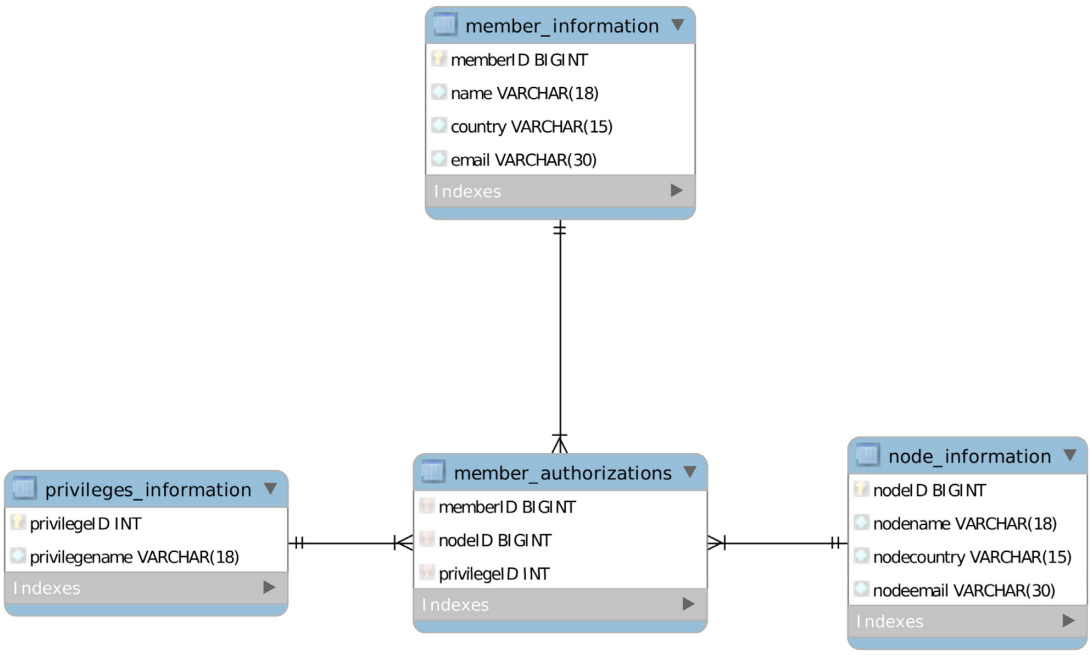

Figure 3: Entity relationship diagram of the logistics node's database. A double bar into an entity indicates a source entity can map to only one entity whereas a trident indicates a source entity can map to many entities. This database contains only member information.

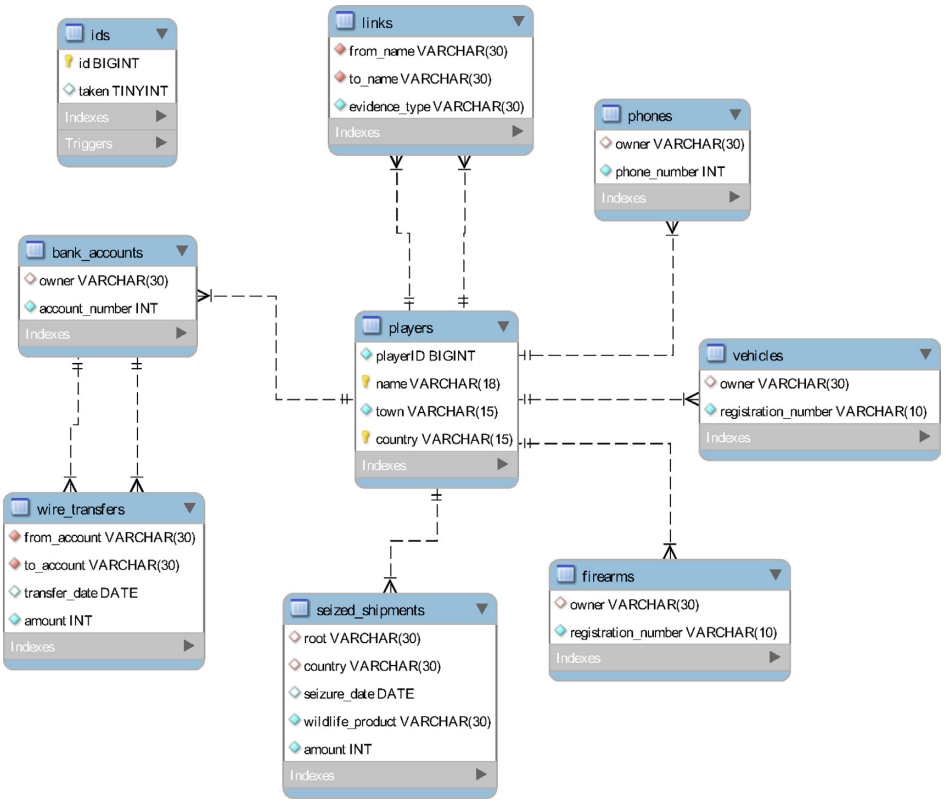

Figure 4: Entity relationship diagram of the database that runs on each node of the confederation's database. See Fig. 3 for the link symbol legend.

Controlling database access

Law enforcement agencies hesitate to share their intelligence mainly because of individual officer unwillingness and an organizational culture that views intelligence sharing negatively [41]. Trust by organization A toward organization B builds over many interactions through time between A and B wherein what B says they will do turns out to be what B actually does. Trust is easily broken: If B intentionally misleads A just once, A will lose trust in B for a long time. This is particularly true when A and B are intelligence agencies [29]. Throughout these interactions, A and B may enjoy a congenial relationship

on the surface. For instance, after then US President Trump revealed items of Israeli security intelligence to the Russians, the Israelis quietly changed their protocols for sharing security intelligence with the USA [72]. These negative attitudes toward intelligence sharing stem in-part from a concern that once released, intelligence may fall into the wrong hands—and there is no way for a node (in the case of a confederation) to prevent this from happening once they release the requested intelligence.

Nodes, however, need to trust members enough to share the names of players and associated intelligence. Simply *de-identifying* players before sharing information on them [73] overcomes this reluctance to share but renders the confederation useless. This is because without the use of shared names across nodes, accurately reconstructing a WTS network would be difficult—increasing the likelihood that key players are omitted from the Detain and Surveil lists. Worse, if player names in these lists are encrypted, they would be useless since law enforcement would have no way of knowing who the confederation recommends to detain or serveil. Because of these two reasons, a node that is distrustful of a particular member, can only opt-out of contributing intelligence to that member's query. But if all nodes opt-out of every query, the confederation has nothing to offer law enforcement for purposes of disrupting a WTS.

Lefebvre [29] finds that the most productive trust relationship among intelligence agencies is bilateral rather than multilateral. The GLAD access control tool described next tempers a bilateral trust relationship within a node–member pair if a second node reports that the member is not to be trusted. This protocol for intelligence sharing is more conservative than the one used by RISS [50].

The GLAD access control tool

This tool 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. The tool consists of three modules: A *local security* module that specifies the local authorization policy of each node; a *global security* module that runs algorithms developed by the authors to combine all exported local authorizations into global ones; and a *dictionary* module that executes operations on nodes as per requests from members who are authorized to do so. 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.

The logistics node stores a copy of each node's local table of member authorizations along with the global authorizations table. The global security module, maintained on the logistics node, runs whenever any node updates their local authorizations table. This global update procedure is as follows (parenthetical SQL scripts appear in Table 1).

(1) Say that at some point, node 2 decides that one or more members need to have their privileges changed. They do this by first, editing an SQL script template that lists these new privileges and then second, emailing this SQL script to the logistics node (required_changes.sql).
(2) The logistics node administrator runs this emailed SQL script against the logistics node's database and then, based on all of these updated per-node member authorization tables, runs a second SQL script that produces an updated global authorizations table (compute_glad.sql). This table encodes the strictly conservative access authorization strategy of the GLAD access control tool.
(3) Next, the logistics node administrator runs a third SQL script (update_privileges.sql). By reading the updated global authorizations table, this SQL script creates a fourth SQL script that the logistics node administrator emails to each node asking them to run it against their local database (global_privileges.sql). When run on a node, this fourth SQL script first removes all privileges on all members, and then issues SQL GRANT commands as necessary to give each member their global authorizations on that node's database.
(4) Finally, node 2 delivers a report to all members that justifies the changes they made to member privileges. Upon receipt of this report, all members vote to accept the report. If <90% of the members accept the report, node 2 is removed from the confederation and the authorizations of the member(s) in question are restored to their former levels.

For example, if the old policy granted UPDATE, and SELECT privileges to a particular member but now, node 2 has shortened this list to only SELECT, the new set of global privileges for that member is SELECT alone. Hence, because the global authorization update procedure runs every time any node updates its local authorizations, when a member runs a query against each node, he/she will acquire only that data that he/she is authorized to acquire under his/her set of global authorizations.

Security advantages of the GLAD access control tool

As a condition of continued confederation membership, all nodes would need to agree to maintain member privileges on their local databases via the GLAD access control tool. Nodes would be motivated to agree to this condition because once a node discovers a security breach and updates their local authorization table accordingly, all other nodes are immediately protected against this breach. Further, the reporting requirement of Step 4 keeps all members up to date on security threats to the confederation's database.

If a node, after emailing the logistics node a list of required changes to the privileges of one or more members, does not quickly receive the expected return email, that node would know that the logistics node has been compromised and hence would immediately remove themselves from the confederation. This fail-safe procedure provides an ongoing diagnostic on the reliability of the logistics node and the GLAD access control tool that it is charged with administering.

This node-driven update protocol ensures that the security concerns of nodes are accurately reflected in their set of local authorizations and in the set of derived, global authorizations. Further, this protocol enforces *full authorization autonomy* wherein the global security module makes no modifications to local authorizations before using them to update global authorizations. Hence, a node does not surrender any control over who may access their data when they join a federated database that is secured by this implementation of the GLAD access control tool.

Another fail-safe feature of the GLAD access control tool is that a member bent on leaking confederation intelligence would need all nodes to grant him/her the SELECT privilege before they could do so. On the other hand, a single malicious node could remove all authorizations in their local security module from every member in order to deny all members access to the confederation's database. Step 4 of the GLAD access control tool guards against this second type of an *insider threat* [74].

A node may have individuals who are not members but have sufficient privileges to modify, insert data into, and delete data from that node's database. Such individuals would have no access to databases maintained by other nodes. But conversely, would not have their local privileges managed by the GLAD access control tool.

Data set formation and WTS network parameter estimation

To build an actionable intelligence report at time t_0, a member queries the confederation's database for two data sets. The first, labeled $D_{t_{current}}$ consists of intelligence acquired over the interval $(t_{\text{current}} - t_{\text{SNA}}, t_{\text{current}})$. The second, labeled $D_{t_{current}-t_{\text{SNA}}}$ consists of intelligence acquired over the interval $(t_{\text{current}} - 2t_{\text{SNA}}, t_{\text{current}} - t_{\text{SNA}})$. The value of t_{SNA} is the amount of time that the network needs to evolve new leaders after law enforcement has disrupted its operations. Limited experience with a real criminal network suggests t_{SNA} should be no >6 months [75]. A player or link is included in a data set only if some activity on the player or link is observed in that data set's observation interval. These player and link expiration rules are needed because players have a high mortality rate [76].

Next, using a method given by Haas and Ferreira [32], each of these networks is reconstructed with a deduplicated network data set (see below) by estimating a set of *hidden links*, and each player's level. Observed links based on messages are weighted by call frequency, links based on wildlife product shipments are weighted by shipment size, and links based on wire transfers are weighted by the USD amount of the transfer. Because these are unimodel social networks, links can be estimated between any two players be they individuals, shipping ports, or bank accounts. These two reconstructed networks are then used to compute the SNA-based components of the actionable intelligence report.

Deduplication of WTS network data

Before data queried from the confederation's database can be used to reconstruct a WTS network, deduplication algorithms need to be run to discover pairs of players in the database who are, in reality, the same person. The primary concern here is that such duplication is the result of players using assumed identities in different countries in an attempt to hide their identities from law enforcement. Nodes in different countries would tend to enter intelligence on such players into their local databases using these assumed identities. Hence, a major advantage of building a federated database of intelligence on an international WTS can be hamstrung unless there is a way to discover those players attempting to hide from law enforcement through the use of assumed identities.

Of course, there are other, non-evasive reasons why duplicates may be present in the database. These include (a) data entry errors due to human mistakes or data migration from different databases; (b) the use of default values on attributes that are not observed; and (c) different nodes entering names that vary in their spelling [77, 78].

After a member has executed a query against the confederation's database that has generated a file containing the requested data, he/she searches for duplicates by running the **id** relation {[46], Chapter 5} deduplicate_players on this file. The algorithm employed is as follows.

(1) Compute *attribute similarity measure* values for all player pairs on the attributes of name and town. Attribute similarity is computed with a measure based on the Levenshtein distance [79]. Also, compute *relational similarity measure* values using each player's contacts and vehicles relations. Do this by computing for a pair of players, two *Jaccard similarity index* values [80]: one using those contacts that the pair has in common, and one using those vehicles that the pair has in common.
(2) Using the attribute, and relational similarity measures computed in the previous step, compute for the i, j^{th} pair of players, the total similarity score $s_{total}(i, j) = \sum_{k=1}^{4} s_k(i, j)$, where $s_k(i, j)$ is their k^{th} similarity measure.
(3) Declare a pair to be a duplicate if their total similarity score exceeds a threshold value, e.g. 0.9.

Running this algorithm produces a list of players who are duplicated across the database—either within database nodes or between them. Bhattacharya and Getoor [81] call the use of relational similarity measures in the computation of $s_{\text{total}}()$, a *naive relational entity resolution scheme*.

Effects on WTS operations

The simulator is an agent-based model of all groups affecting the at-risk ecosystem as described in ref. [54]. A submodel is constructed for each player level. These are called *WTS submodels*. Each of these agents make risk–benefit assessments as they weigh different actions that they might take. These agents receive input actions such as wildlife product requests and law enforcement operations. Given these inputs, they implement actions that include poaching, wire transfers, and wildlife product shipments.

The WTS network is embedded in the simulator by having an individual level-i player implement the action computed by a level-i WTS submodel, $i = 1, \ldots, 4$ (poacher, middleman, trader, retailer). Thus, player decision making is simulated with group decision making submodels that capture the unique goals and audiences that a player at a particular level is using to make decisions.

An example of this embedding is the modeling of a direct effect on plant/animal abundance with the following causal chain.

> A particular retailer pays a particular trader → this trader pays a particular middleman → this particular middleman pays a particular poacher → this particular poacher poaches l plants/animals of an endangered species → the ecosystem submodel reduces abundance of the targeted species by the amount l.

In this chain, the poacher submodel executes a poaching action only if a request for wildlife products by a middleman is the input action to the poachers submodel. Otherwise, poaching is not the output action. Removing all traders breaks this chain because in this case, there are no requests for wildlife products——and hence, no poaching events.

This particular synthesis of agent-based modeling and social networks is new. Its agent-based foundation predates a like approach taken by ref. [49] in their modeling of the effect of US interdiction raids on the expansion of a Central American cocaine trafficking syndicate.

The simulator's disaggregation procedure

To implement this embedding, a disaggregation procedure is needed because a WTS submodel is an aggregated model of a group's decision making wherein it is assumed that one un-named member of group actually implements the output action computed (chosen) by the submodel. This group member is selected as follows.

Let n_i be the number of level-i players in the confederation's database at time t_0. Select a player as follows.

(1) If $n_i = 0$, do not select a player. In this case, the WTS submodel does not post any action.

(2) If a player is named in an observed action, use that player.
(3) If an observed action is location-specific, randomly choose a player from that location.
(4) Otherwise, randomly select a player from the set of all players who are at the submodel's level, e.g. if the trader submodel is to post an action, randomly select a trader-level player. Let the selection probability for the j^{th} player in level-i, be $p^{(ij)}_{\text{select}} \equiv \xi_{ij}/(\sum_{k=1}^{n_i} \xi_{ik})$, where ξ_{ij} is player ij's eigenvector centrality.

Effects of player removals

The simulator is used to assess future effects on an ecosystem due to the removal of particular sets of players. To this end, the statistically fitted simulator is run over a future time period, $(t_{\text{current}}, t_{\text{end}})$, where t_{current} is the current (present) time. At each time point in this period, each level-i WTS submodel first computes an output action, and then selects a level-i player to implement it using the above, 4-step procedure.

Let $m_i \leq n_i$, $i = 1, \ldots, 4$ be the number of level-i players that are recommended by the confederation for removal. Let the total number of players removed be $m \equiv \sum_{i=1}^{4} m_i$. Working with law enforcement, a feasible time is found for this removal operation. Call this time point, $t_r \in (t_{\text{current}}, t_{\text{end}})$. A set of m players to remove is found by randomly selecting m players from the current list of active players in the confederation's database regardless of their level, SNA measures, or attribute values.

Effects on WTS operations due to the removal of a particular set of m_1 poachers is as follows. As recorded in the confederation's database, let β_j be the number of times poacher j has participated in a poaching raid. Let $\hat{\beta}$ be the average of this value over all poachers in the confederation's database. Let $\hat{\beta}_r$ be the average of this value over the set of m_1 poachers selected for removal. When the poacher submodel decides to *poach some plants/animals*, this event is not implemented in the IBM with probability $\min\{1,\ m_1\hat{\beta}_r/[\hat{\beta}(n_1 - m_1 + 1)]\}$.

This mechanism represents the hypotheses that (a) the more poachers, the less effect the removal of m_1 of them has on the event *poach some plants/animals*; and (b) the prowess of an individual poacher is captured by how many poaching raids he/she has been on. Because there are so many poachers, the best that law enforcement can hope for is to stop a single, planned poaching raid by removing those poachers who would most likely have successfully executed their next planned poaching raid. Modeling a pause in poaching due to the removal of a few poachers is unrealistic because of the large number of poachers, their high recruitment rate, and their wide dispersal around the borders of many wildlife reserves in developing countries.

Effects on WTS operations due to the removal of a particular set of m_2 middlemen, m_3 traders, and m_4 retailers is as follows. Drawing from the confederations database, let a_j be the number of times middleman, trader, or retailer j has been arrested. Let b_j be the number of wildlife product shipments linked to middleman, trader, or retailer j. Let f_j and v_j be middleman, trader or retailer j's number of firearms, and vehicles, respectively. Let $\alpha_j = a_j + b_j + f_j + v_j$. Let $\hat{\alpha}_i$ be the average value of α over all middlemen ($i = 2$), traders ($i = 3$), or retailers ($i = 4$) in the confederation's database. Let $\hat{\alpha}^{(i)}_r$ be the average value of α over the selected set of m_i middlemen, traders, or retailers to remove. The removal operation causes the middlemen, traders, or retailers submodel to not post actions during the time period $(t_r,\ t_r + t_{d_i})$, where $t_{d_i} = \hat{\alpha}^{(i)}_r/[\gamma\hat{\alpha}_i(n_i - m_i + 1)]$. During this delay, if $i = 4$, retailers do not offer to purchase wildlife products from traders; if $i = 3$, traders do not request wildlife products from middlemen; and if $i = 2$, middlemen do not request poachers to poach members of the targeted species.

The hypotheses that this delay interval represents are (a) the more level-i players, the quicker the network can recover from a removal operation; and (b) the interval's length is proportional to the length of a player's criminal record, the amount of business he/she has recently transacted, the number of firearms linked to them, and the number of vehicles linked to them. This mechanism leverages the information contained in the network's resiliency index.

Keeping t_r fixed, the optimal removal algorithm (Appendix) randomly selects a set of m players to remove each time it re-runs the simulator over $(t_{\text{current}}, t_{\text{end}})$. Hence, each such removal set results in potentially different impacts on the plant/animal population that in-turn, lead to different expected plant/animal abundance values at time t_{end}.

Results

Methods developed above are applied to the political–ecological system that encompasses rhino horn trafficking. An early model of this system [82] contains submodels of poachers, antipoaching forces, middlemen, horn consumers, and an individual-based model (IBM) of the KNP rhino population. This model is enlarged by adding to it a traders submodel; and a submodel of those retailers operating in countries where rhino horn is consumed. The path taken by a rhino horn in this model is:

IBM → poachers → middlemen → traders → retailers → consumers.

A hypothetical example is described next that illustrates the workings of the confederation described above. See ref. [83] for all files employed in this example.

A hypothetical WTS

Say that in reality, there exists a WTS network as shown in Fig. 5. Table 2 contains this network's centrality measures.

Because player t1 has a high ratio of betweenness centrality to degree centrality, this player may be attempting to hide his/her importance to the WTS.

A confederation has managed to gather some intelligence on this WTS (Table 3). The confederation controls access to the database that holds this intelligence with the GLAD access control tool wherein the authorization strategy has been set to *strictly conservative*.

Controlling access to intelligence

Member John Doe has been enjoying full access privilege by all nodes. But recently, node 2 has learned that John Doe is adding false information to the confederation's database. This knowledge has led node 2 to revoke John Doe's INSERT privilege. Node 2 does this by emailing an SQL script to the logistics node (Fig. 6). Upon receipt of this email, the logistics node administrator updates John Doe's GLAD authorizations on all nodes (Figs 6 and 7). At some later time, John Doe submits a query against the confederation's database that attempts to add a new phone number to player m3 (example_query.sql). This query fails because GLAD's strictly conservative authorization strategy uses the lowest level of data access authorizations for this user across all nodes—and that lowest level is the set of privileges dictated by node 2 (Fig. 6).

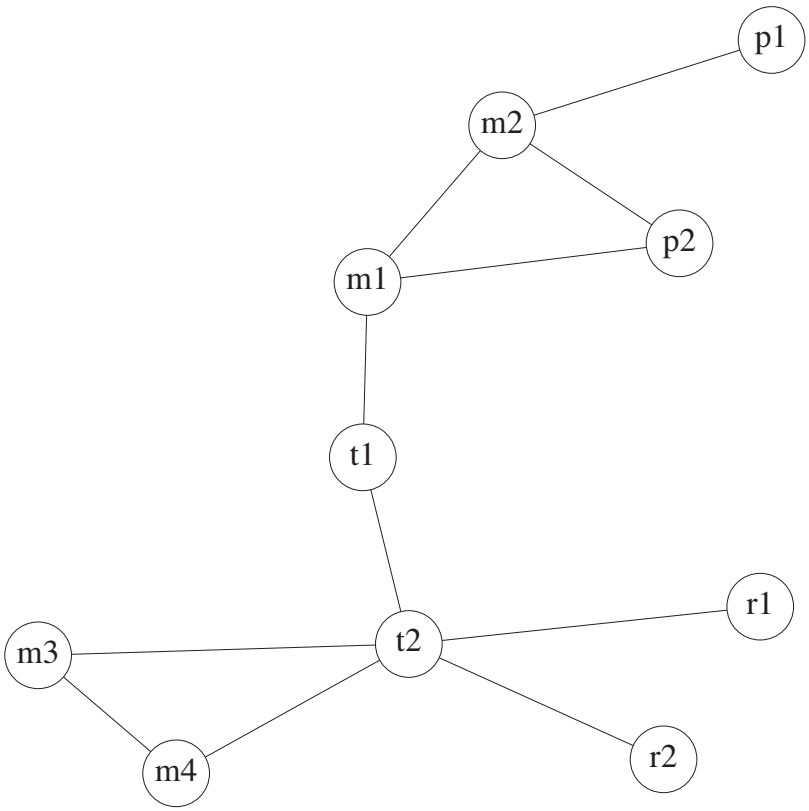

Figure 5: A hypothetical WTS. Poacher names begin with "p," middlemen with "m," traders with "t," and retailers with "r."

Table 2: Centrality measures of the actual WTS network.

Player	Eigenvector	Betweeness	Degree	Betweenness/degree
t2	0.552	68	5	13.6
m4	0.361	18	2	9.0
m3	0.361	18	2	9.0
t1	0.352	58	2	29.0
m1	0.300	54	3	18.0
m2	0.244	34	3	11.3
r2	0.228	18	1	18.0
r1	0.228	18	1	18.0
p2	0.216	18	2	9.0
r1	0.092	18	1	18.0

Values are computed with the **id** relation report evaluate evaluate_network().

This example shows that a single node is able to reduce a member's access to the confederation's database.

Deduplicating players

The intelligence contains the player t11 who in reality, is player t1 (Table 3). The deduplication algorithm (section "Deduplication of WTS network data") is run on this intelligence with the threshold parameter set to 0.5. This duplication is detected (Fig. 8).

Actionable intelligence

SNA computations

First, the WTS network is reconstructed with this deduplicated intelligence using the following **id** relation

Table 3: Intelligence gathered on players.

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

	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

Top: player attributes. Bottom: player-to-player interactions.

```
************** 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

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

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
```

Figure 6: Trace of a GLAD access control tool update that is initiated by node 2 via the SQL script required_changes.sql.

report estimate reconstruct_social_network(players.dat 1 1000).

This reconstructed network is used to find those players who should be removed according to social network theory. This is accomplished by running the relation

report evaluate evaluate_network()

on the intelligence file player.dat wherein t11 has been removed. These players form the first sublist of the Detain list in the confederation's actionable intelligence report (Figs 10 and 11).

The report's recommended sequence of arrests [32] implement the idea that the network's kingpin (highest eigenvector centrality) should be removed first followed by the network's central information broker (highest betweenness centrality). This sequence

```
************** 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)

************** 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'
```

Figure 7: SQL script emailed to every node followed by the trace of the query (example_query.sql) against the confederation's database executed by a member who is not trusted by node 2, namely, John Doe.

```
report estimate deduplicate_players(players.dat 0.5)

-----------------------------------------------------------

                      id
       Influence Diagram Construction,
      Estimation, and Evaluation System
        written by Timothy C. Haas
      Sheldon B. Lubar College of Business
      University of Wisconsin-Milwaukee
      P.O. Box 742, Milwaukee, WI 53201
                haas@uwm.edu
               February 2022.

h6 and h11 ts= 0.542 are predicted to be duplicates.
runtime= 00.03 seconds, or 00.00 minutes
Normal termination of id
```

Figure 8: The **id** deduplication relation (above dashed line), and its output (below dashed line).

of arrests is designed to first remove the network's leader before the network has time to hide him or her—and then cripple the network's communications by removing its most important communicator.

This relation also generates a run of the Raghavan *et al.* [59] community discovery algorithm. This run returns two communities: {t1, t2, r1, r2, m3, m4} and {m1, m2, p2, p1}. These communities are intuitively consistent with the network's connectivity (Fig. 5).

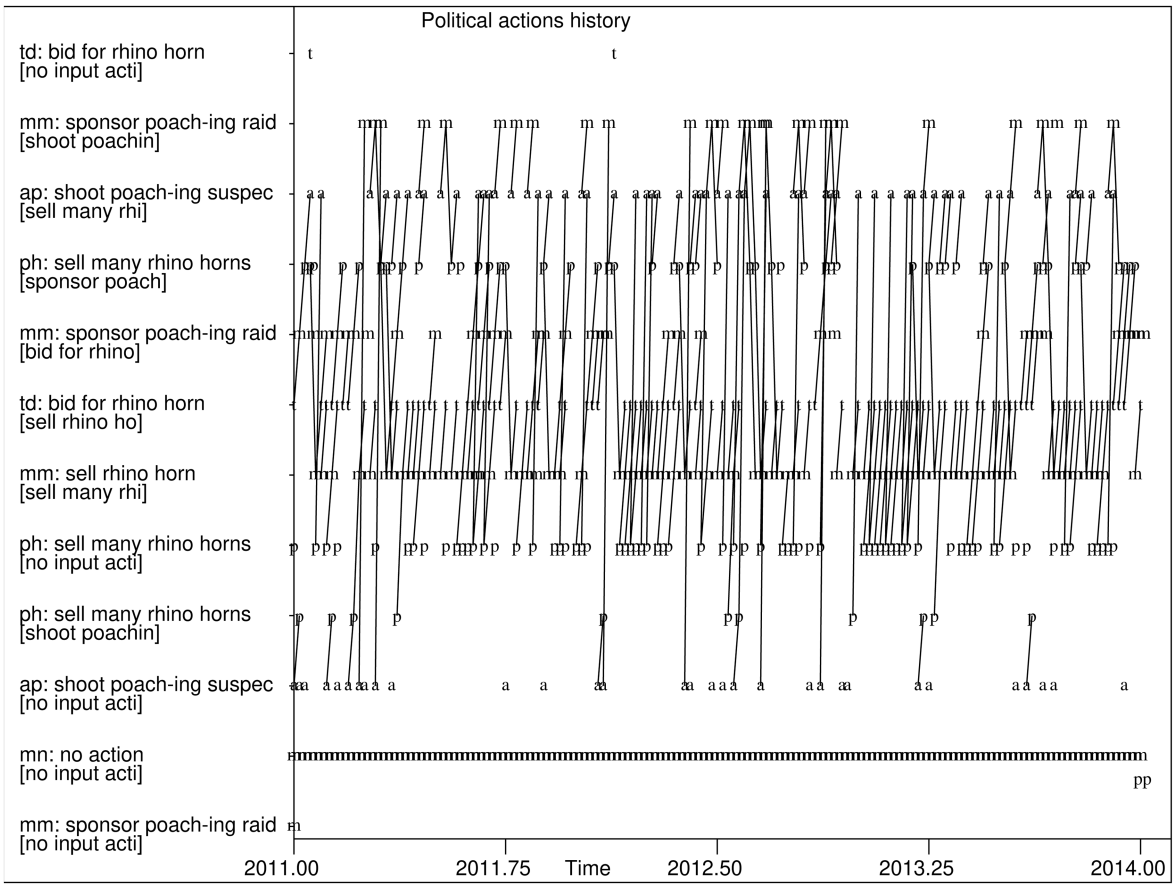

Figure 9: Actions history generated by the fitted simulator. Plotting symbols are t: trader, m: middleman, p: poacher, and a: antipoaching unit.

Simulator computations

Next, an observed actions history is collected and used to estimate the simulator's parameters. The actions history generated by this fitted simulator (Fig. 9) exhibits a re-occurring *episode* [67]: *traders bid for rhino horn*—then *middlemen sponsor poaching raid*— then *poachers sell many rhino horns*—then *middlemen sell rhino horns*.

This fitted simulator is used by the optimal removal algorithm to find the three players whose removal will reduce the poaching rate the most. These players are added to the Detain list. The relation that performs this search is

```
report evaluate remove_players(3 1),
```

where $m = 3$, and $r = 1$ (Appendix). During this search, the highest average number of poached rhinos was 1560. The algorithm converged after 209 function evaluations to a solution that gave the smallest number of poached rhinos (488) by removing players t1, p2, and m1 on 1 January 2012 over the study interval (1 January 2011, 1 January 2014). t1 is the only player who owns a vehicle.

Actionable intelligence report

The confederation sends its actionable intelligence report (Figs 10 and 11) to law enforcement. The report recommends that the WTS kingpin, t1 be arrested. In particular, reflecting the reality of this WTS, the report identifies player t1 as someone attempting to hide his/her importance to the WTS since this player has a high ratio of betweenness centrality to degree centrality. t1 may be acting as a liaison between the network's two communities.

The most recent interdictable actions in the actions history are used to build the Interdict list. Here, this the single action *middlemen sell rhino horn*. Middleman m3 is predicted to execute this action. Because this player is located in town B, country Y, the confederation recommends a stake-out operation be planned to intercept this sale at that location.

Discussion

A functioning confederation as developed herein would have direct and measurable impacts on biodiversity conservation. Several challenges, however, remain.

Corrupt officials may impede a confederation's operations

Sections "Evaluating candidates for confederation membership" and "Controlling database access" discuss one way to stop corrupt confederation members from undermining the confederation's operations. But there is another source of corruption effects on a confederation: Government officials outside of the confederation who work in law enforcement, prosecution, and the judiciary. These officials may be persuaded by trafficker bribes, intimidation, political pressure, or conflicts of interest to drop wildlife trafficking investigations {[84], Page 4}. In the worst case, these officials may shutdown those investigations being pursued by a confederation and stop the confederation's efforts to disrupt a WTS. Legislation outlawing governmental corruption, however, may not always be effective. For example,

```
           ACTIONABLE INTELLIGENCE REPORT

---------- Social Network Analysis Metrics -------------
 Player  Eigenvector  Degree      Predicted
         Centrality   Centrality  Level
    t2        00.552       5.000    3
    m4        00.361       2.000    2
    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
    r1        00.228       1.000    4
    p2        00.216       2.000    1
    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

           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
```

Figure 10: Actionable intelligence report.

Koehler [85] finds that the Foreign Corrupt Practices Act (FCPA) has a mixed record in reducing the amount of bribery that US businesses need to engage in to conduct business in many countries.

A confederation could employ several strategies to ward off these attacks including the following.

(1) The confederation could call upon governments of those countries who are able to influence the government employing these corrupt officials. Such influence would take the form of diplomatic contacts, economic inducements, or sanctions. Recent evidence suggests that international businesses are joining private *anti-bribery* clubs that give government officials incentives to forgo bribes before they provide governmental services to these businesses [86]. Confederation members should join such clubs in those countries where they are pursuing wildlife trafficking investigations.
(2) Using the example of the bribes paid by Oskar Schindler to the Nazis to spare the lives of a group of Jews (the so-called *Schindlerjuden*), Nichols [42] argues that there is one case where a bribe is justified: When a human life cannot be saved any other way. A similar argument could be made to justify a confederation's use of bribes to allow wildlife crime investigations to continue.
(3) A confederation should avoid relationships that give a government some amount of control over it. For instance, a confederation should avoid housing its logistics office on government property, and avoid using a government's IT hardware, software, and support staff.

The challenge of leaked/inadmissible intelligence

A procedure based on the GLAD access control tool has been described for how a confederation would maintain the confidentiality of its intelligence. Even so, there would be nonzero risks associated with (a) leaked intelligence causing a violation of a targeted suspect's right to privacy, and (b) intelligence being declared inadmissible in court due to inappropriate collection methods and/or leaks.

One way a confederation could protect itself against legal attacks by players aimed at suppressing investigations into possible wildlife crimes, is to maintain a fund to fight lawsuits brought by players against members for alleged breach of privacy, inadmissible evidence, or libel stemming from confederation investigations. This fund would support the services of law firms specializing in environmental law. Such firms include the Southern Environmental Law Center (SELC) [87].

The challenge of uneven wildlife crime legislation

Transnational wildlife crime investigations may also encounter difficulties in supporting successful prosecutions because of differing

```
-------------------- 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 algorithm iterations: 2
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

----------------- 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.
```

Figure 11: Actionable intelligence report, continued.

wildlife crime legislation across countries. A recent United Nations report explains that

> Wildlife crime related to CITES trade violation is clearly defined by CITES requirements, but outside trade violations, wildlife crime varies from country to country and some actions involving wildlife may be a criminal offence in one country but not in another {[8], Page 89}.

A prominent example of this difficulty is the potential reversal of the ban on rhino horn trading in China. At the moment, this ban is in-place but could be lifted at any time [43]. If this ban is lifted, how will it be possible for instance, to prosecute a Chinese rhino horn retailer?

At its heart, this is an international politics issue in that what is needed is a harmonization of wildlife crime laws across countries.

Differences from Interpol

The proposed confederation is qualitatively different than Interpol. These differences include the following.

(1) The proposed confederation would focus on the collection and analysis of wildlife trafficking intelligence.
(2) The proposed confederation would issue only *specific* recommendations to law enforcement: arrest, surveil, or interdict.
(3) The proposed confederation's database would be federated rather than controlled by a single entity {[52], Page 61}. Interpol's General Secretariat makes closed-door decisions on what data may or may not be included in its databases [88].
(4) Any confederation member could unilaterally block any other member's access to the confederation's database.
(5) The proposed confederation would be nonhierarchical, i.e. it would have no president and no governing board.
(6) The proposed confederation would only issue notices in the form of actionable intelligence reports that are created out of its own analysis of its own intelligence. Interpol's practice of issuing *red notices* that are not required to carry evidential support from Interpol data can lead to accusations of corruption. Specifically, that such notices are being issued to intimidate critics of authoritarian regimes [89, 90].
(7) A member can be voted out of the confederation as a result of loss of trust or the perception by a majority of the confederation's members that he/she is using the confederation for political gain. On the contrary, Toby Cadman, a British barrister working on Syria-related war crimes prosecutions, notes that "Interpol's systems are opaque, with no real oversight or accountability, and routinely abused by states like Syria." [91].

Future work

The detection of overlapping communities in a WTS network would increase the realism of the network's predicted community structure because criminal communities, being social systems, have players who act as liaisons between communities and hence, belong to more than one community. This could be accomplished with the algorithm of Lu *et al.* [92].

Currently, the simulator's submodels do not include spatial location. As intelligence on player locations is gathered, the simulator could be fitted to intelligence on player actions that are spatio-temporally indexed. Doing so would allow the fitted simulator to produce spatio-temporal predictions of actions by particular players.

Such predictions would result in more interdiction operations that successfully intercept the predicted wire transfer or wildlife product shipment.

A necessary step toward implementing a confederation in the real world is to survey law enforcement professionals to find out what they think of this proposed confederation.

Supplementary data

Supplementary material is available at *Cybersecurity Journal* online.

Acknowledgments

The author thanks two anonymous reviewers for comments that improved the manuscript.

Author contributions

Timothy C. Haas (Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Resources, Software, Validation, Visualization, Writing – original draft, and Writing – review & editing).

Conflict of interest statement

The author declares that there is no conflict of interest.

Funding

No external funding sources to declare.

REFERENCES

1. INTERPOL. Who will police Interpol?. *INTERPOL*, 2020. https://www.interpol.int/en/News-and-Events/News/2020/Wildlife-and-forestry-crime-Worldwide-seizures-in-global-INTERPOL-WCO-operation (15 March 2023, date last accessed).
2. IUCN. African elephant species now endangered and critically endangered - IUCN Red List. *International Union for the Conservation of Nature* 2021. https://www.iucn.org/news/species/202103/african-elephant-species-now-endangered-and-critically-endangered-iucn-red-list (7 April 2022, date last accessed).
3. Njini F. White rhino numbers may have fallen 24%, foundation says. *Bloomberg Green*, 21 September 2021. https://www.bloomberg.com/news/articles/2021-09-21/white-rhino-numbers-may-have-fallen-24-foundation-says (7 April 2022, date last accessed).
4. Ellis-Petersen H. Vietnam seizes 125 Kg of smuggled rhino horns worth $7.5m. *The Guardian*, 29 July 2019 https://www.theguardian.com/world/2019/jul/29/vietnam-seizes-125kg-of-smuggled-rhino-tusks-worth-75m (8 July 2021, date last accessed).
5. BBC. Hong Kong seizes $1m worth of rhino horn at airport. BBC News, 15 February 2019. https://www.bbc.com/news/world-asia-china-47258340 (8 July 2019, date last accessed).
6. Frank EG, Wilcove DS. Long delays in banning trade in threatened species. *Science* 2019;**363**:686–88. https://www.science.org/doi/10.1126/science.aav4013 (17 January 2023, date last accessed).
7. Morton O, Scheffers BR, Haugaasen T. *et al.* Impacts of wildlife trade on terrestrial biodiversity. *Nat Ecol Evol* 2021;**5**:540–8.. https://www.nature.com/articles/s41559-021-01399-y (17 January 2023, date last accessed).
8. UN. United Nations office on drugs and crime. ISBN: 978-92-1-148349-9. *World Wildlife Crime Report*, 2020. https://www.unodc.org/documents/data-and-analysis/wildlife/2020/World_Wildlife_Report_2020_9July.pdf (8 July 2021, date last accessed).
9. Scheffers BR, Oliveira BF, Lamb I. *et al.* Erratum for the research article: "Global wildlife trade across the tree of life by B. R. Scheffers, B. F. Oliveira, I. Lamb, D. P. Edwards". *Science* 2020;**369**:eabd8164. https://www.science.org/doi/10.1126/science.abd8164 (17 January 2023, date last accessed).
10. Lavorgna A, Sajeva M. Studying illegal online trades in plants: market characteristics, organisational and behavioural aspects, and policing challenges. *Eur J Crim Policy Res* 2021;**271**:451–70. https://link.springer.com/article/10.1007/s10610-020-09447-2 (17 January 2023, date last accessed).
11. Tittensor DP, Harfoot M, McLardy C,. *et al.* Evaluating the relationships between the legal and illegal international wildlife trades. *Conserv Lett* 2020;**13**:e12724. https://conbio.onlinelibrary.wiley.com/doi/full/10.1111/conl.12724 (17 January 2023, date last accessed).
12. Fears D. Overwhelmed U.S. port inspectors unable to keep up with illegal wildlife trade. *The Washington Post*, 17 October 2014. https://www.washingtonpost.com/national/health-science/overwhelmed-us-port-inspectors-unable-to-keep-up-with-illegal-wildlife-trade/2014/10/17/2fc72086-fe42-11e3-b1f4-8e77c632c07b_story.html (17 January 2023, date last accessed).
13. Wyatt T, Maher J, Allen D. *et al.* The welfare of wildlife: an interdisciplinary analysis of harm in the legal and illegal wildlife trades and possible ways forward. *Crime Law Soc Change* 2022;**77**:69–89. https://link.springer.com/article/10.1007/s10611-021-09984-9#Abs1 (18 January 2023, date last accessed).
14. Hanski I. Habitat loss, the dynamics of biodiversity, and a perspective on conservation. *Ambio* 2011;**40**:248–55. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3357798/(18 January 2023, date last accessed).
15. Jaureguiberry P, Titeux N, Wiemers M. *et al.* The direct drivers of recent global anthropogenic biodiversity loss. *Sci Adv* 2022;**8**:eabm9982. https://www.science.org/doi/pdf/10.1126/sciadv.abm9982 (16 January 2023, date last accessed).
16. Platt JR. Let's put more effort into investigating and prosecuting environmental crimes. *The Revelator*, 9 May 2022. https://therevelator.org/eco-detectives/ (17 January 2023, date last accessed).
17. DEA. State and local task forces. Drug Enforcement Administration, 1 January 2023. https://www.dea.gov/operations/state-and-local-task-forces#::text=These%20task%20forces%20are%20staffed,2%2C500%20state %20and%20local%20officers. (18 January 2023, date last accessed).
18. Smith JE. Illegal wildlife trade overwhelms federal enforcement, likely unstoppable without increased public awareness. The San Diego Union-Tribune, 22 April 2018. https://www.sandiegouniontribune.com/news/environment/sd-me-wildlife-trafficking-20180418-story.html (17 January 2023, date last accessed).
19. Surugue L. The fight to bring a deadly illegal industry to justice. BBC Future, 24 September 2019. https://www.bbc.com/future/article/20190920-the-fight-to-end-wildlife-crime-and-poaching (8 July 2021, date last accessed).
20. Ceballos G, Ehrlich PR, Barnosky AD. *et al.* Accelerated modern human-induced species losses: entering the sixth mass extinction. *Sci Adv* 2015;**1**:e1400253.
21. de Vries S. The necessity of cooperation in criminal wildlife matters: a case study of the challenges faced and cooperative mechanisms available to Canadian wildlife officials. *J Int Wildl Law Policy* 2021;**24**:268–90. https://www.tandfonline.com/doi/full/10.1080/13880292.2021.2019380?scroll=top&needAccess=true&role=tab (17 January 2023, date last accessed).
22. Jiao Y, Yeophantong P, Lee TM. Strengthening international legal cooperation to combat the illegal wildlife trade between Southeast Asia and China. *Front Ecol Evol* 2021;**9**:645427. https://www.frontiersin.org/articles/10.3389/fevo.2021.645427/full (18 January 2023, date last accessed).
23. Bertrand AA. The link between corruption and illegal wildlife trafficking. *UNCAC Coalition*, 24 March 2021. https://uncaccoalition.org/corruption-and-illegal-wildlife-trafficking/ (18 January 2023, date last accessed).
24. Neme L. Journey to oblivion: unraveling Latin America's illegal wildlife trade. *Mongabay*, 16 November 2015. https://news.mongabay.com/2015/11/journey-to-oblivion-unraveling-latin-americas-illegal-wildlife-trade/ (16 January 2023, date last accessed).

25. Youd F. Helping the maritime industry spot wildlife crimes. *Ship Technology*, 29 July 2021. https://www.ship-technology.com/features/helping-the-maritime-industry-spot-wildlife-crimes/ (16 January 2023, date last accessed).
26. Bose A. Understanding wildlife cybercrime and ways to curb it. *iPleaders*, 2021. https://blog.ipleaders.in/understanding-wildlife-cybercrime-ways-curb/ (10 June 2022, date last accessed).
27. Pipikaite A, Barrachin M, Crawford S. These are the top cybersecurity challenges of 2021. The Davos Agenda, *The World Economic Forum*, 21 January 2021. https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/ (10 June 2022, date last accessed).
28. Axon L, AlAhmadi BA, Nurse JRC. *et al.* Data presentation in security operations centres: exploring the potential for sonification to enhance existing practice. *J Cybersecur* 2020;**6**:1–16.
29. Lefebvre S. The difficulties and dilemmas of international intelligence cooperation. *Int J Intell CounterIntell* 2003;**16**:527–542.
30. Brilingaitė A, Bukauskas L, Juozapavičius A. *et al.* Overcoming information-sharing challenges in cyber defence exercises. *J Cybersecur* 2022;**8**:1–9.
31. Sirait RA, Damayanti T, Hidayat DR. *et al.* Digital intelligence strategy in combatting wildlife trafficking. *J Phys Conf Ser* 2018;**1114**:012091.
32. Haas TC, Ferreira SM. Federated databases and actionable intelligence: using social network analysis to disrupt transnational wildlife trafficking criminal networks. *Secur Inform* 2015;**4**:1. https://link.springer.com/article/10.1186/s13388-015-0018-8 (20 May 2021, date last accessed).
33. Merriam-Webster. Defintion of "Syndicate." *Merriam-Webster Dictionary*, 2021. https://www.merriam-webster.com/dictionary/syndicate (19 May 2021, date last accessed).
34. Newman J. Combating money laundering and the illegal wildlife trade. *Environmental Investigation Agency*, 1 January 2023. https://eia-international.org/wildlife/combating-money-laundering/ (18 January 2023, date last accessed).
35. Mulqueeny KK, Cordon FJJ. (eds.) *Symposium on Combating Wildlife Crime: Securing Enforcement, Ensuring Justice, and Upholding the Rule of Law, The Proceedings*. Mandaluyong City, Philippines: Asian Development Bank, 2014. ISBN: 978-92-9254-791-2. https://www.adb.org/sites/default/files/publication/149395/combating-wildlife-crime-proceedings.pdf (3 June 2022, date last accessed).
36. Allan C, Fischer S. Combatting wildlife trafficking – protecting biodiversity and beyond. *International Airport Review*, May 2021. https://www.internationalairportreview.com/article/158332/combatting-wildlife-trafficking/ (19 January 2023, date last accessed).
37. Costenbader E, Valente TW. The stability of centrality measures when networks are sampled. *Soc Networks* 2003;**25**:283–307.
38. Kossinets G. Effects of missing data in social networks. *Soc Networks* 2006;**28**:247–68.
39. Cruise A. Wildlife trafficking: the sordid connection. The Journal of African Elephants, 10 January 2017. https://www.africanelephantjournal.com/wildlife-trafficking-the-sordid-connection/ (19 January 2023, date last accessed).
40. Wilson-Späth A. Governments are not doing enough to stop wildlife crime. Conservation Action Trust, 4 January 2017. https://conservationaction.co.za/media-articles/governments-not-enough-stop-wildlife-crime/ (19 January 2023, date last accessed).
41. Abrahamson DE, Goddman-Delahunty J. Impediments to information and knowledge sharing within policing: a study of three Canadian policing organizations. *Sage Open* 2014;**4**:1–17.
42. Nichols PM. The good bribe. *The UC Davis Law Review* 2015;**49**:647–84.
43. Phys. China postpones lifting rhino, tiger parts ban. *Phys Org*, 12 November 2018. https://phys.org/news/2018-11-china-postpones-rhino-tiger.html (8 July 2021, date last accessed).
44. Ray JC, Grimm J, Olive A. The biodiversity crisis in Canada: failures and challenges of federal and sub-national strategic and legal frameworks. *FACETS* 2021;**6**:1044–68. https://www.facetsjournal.com/doi/10.1139/facets-2020-0075 (20 January 2023, date last accessed).
45. Webster H. Lies, damn lies, and animal rights activists. *Natural Storytelling*, 11 December 2021. https://hughwebsterauthor.wordpress.com/2021/12/11/lies-damn-lies-and-animal-rights-activists/ (20 January 2023, date last accessed).
46. Haas TC. *Improving Natural Resource Management: Ecological and Political Models*. Chichester: Wiley-Blackwell, 2011.
47. Castano S, De Capitani di Vimercati S, Fugini MG. Automated derivation of global authorizations for database federations. *J Comput Secur* 1997;**5**:271–301.
48. U.S. Department of the Treasury. *Iran Sanctions*. U.S. Department of the Treasury, 2021. https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/iran-sanctions (7 April 2022, date last accessed).
49. Magliocca NR, McSweeney K, Sesnie SE,. *et al.* Modeling cocaine traffickers and counterdrug interdiction forces as a complex adaptive system. *Proc Natl Acad Sci* 2019;**116**:7784–92.
50. RISS. About the RISS program. RISS, 2021. https://www.riss.net/about-us/ (14 July 2021, date last accessed).
51. Gore A. *Our people*. Kenya: Centre for Global Advancement, 2021 . https://globaladvancement.org/about/ (21 July 2021, date last accessed).
52. ECOFEL. *Financial investigations into wildlife crime*. The Egmont Group, January 2021. https://egmontgroup.org/wp-content/uploads/2021/09/2021_ECOFEL_-_Financial_Investigations_into_Wildlife_Crime.pdf (21 July 2021, date last accessed).
53. van Uhm D, South N, Wyatt T. Connections between trades and trafficking in wildlife and drugs. *Trends Organ Crime* 2021;**24**:425–46.
54. Haas TC. Developing political-ecological theory: the need for many-task computing. *PLoS One* 2020;**15**:e0226861.
55. Duijn PAC, Kashirin V, Sloot PMA. The relative ineffectiveness of criminal network disuption. *Sci Rep* 2014;**4**:4238.
56. Ayling J. What sustains wildlife crime? Rhino horn trading and the resilience of criminal networks. *J Int Wildl Law Policy* 2013;**16**:57–80.
57. Nuwer R. *How to stop poaching and protect endangered species? Forget the 'kingpins.'* The New York Times, 24 September 2018. https://www.nytimes.com/2018/09/24/science/poaching-conservation-rhinos-elephants.html (4 June 2022, date last accessed).
58. Security Management. CBP: Taking out cartel leadership has no impact on flow of drugs. *Security Management*, 15 July 2011. https://www.asisonline.org/security-management-magazine/articles/2011/07/cbp-taking-out-cartel-leadership-has-no-impact-on-flow-of-drugs/ (4 June 2022, date last accessed).
59. Raghavan UN, Albert R, Kumara S. Near linear time algorithm to detect community structures in large-scale networks. *Phys Rev E* 2007;**76**:036106.
60. Benowitz P. OFAC blocked property and enforcement. *OFAC Sanctions Attorney*, blog post 2021. https://ofaclawyer.net/enforcement-powers/blocked-property/ (28 May 2021, date last accessed).
61. Paying For Senior Care. *Federal poverty guidelines / federal poverty levels*. Paying For Senior Care, 2 January 2023. https://www.payingforseniorcare.com/federal-poverty-level (19 January 2023, date last accessed).
62. Koch T, Kramer B, Rohde G. On a rule based management architecture. *Second International Workshop on Services in Distributed and Networked Environments*, Whistler, BC, 5–6 June 1995. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=470461 (19 July 2021, date last accessed).
63. Lohmann R A. Break even analysis: a tool for budget planning (revised). *Faculty & Staff Scholarship*, 2020, p. 2585. The Research Repository @ WVU, West Virginia University. https://researchrepository.wvu.edu/cgi/viewcontent.cgi?article=3505&context=faculty_publications (19 January 2023, date last accessed).
64. Williams T. Commentary: Everything comes at a price that must be paid. The NonProfit Times, 28 December 2021. https://www.thenonprofittimes.com/npt_articles/commentary-everything-comes-at-a-price-that-must-be-paid/ (19 January 2023, date last accessed).
65. Linhartová V, Volejníková J. Quantifying corruption at a subnational level. *E M Ekon Manag* 2015;**18**:25–39. https://dspace.tul.cz/bitstream/

handle/15240/9104/EM_2_2015_3.pdf?sequence=1 (19 July 2021, date last accessed).
66. Yusuf SE, Hong JB, Ge M,. *et al*. Composite metrics for network security analysis. *Software Networking* 2017;**1**:137–60. https://www.riverpublishers.com/journal_read_html_article.php?j=JSN/2017/1/007 (19 July 2021, date last accessed).
67. Haas TC. The first political-ecological database and its use in episode analysis. *Front Conserv Sci* 2021;**2**:707088. https://www.frontiersin.org/article/10.3389/fcosc.2021.707088 (7 April 2022, date last accessed).
68. Oracle Corp. MySQL 8.0 Reference Manual. Oracle Corporation, 2022. https://dev.mysql.com/doc/refman/8.0/en/ (9 February 2022, date last accessed).
69. Petković D. *Microsoft SQL Server 2019: A Beginner's Guide Seventh Edition*. New York, NY, McGraw-Hill Education, 2019, 864. ISBN: 978-1260458879.
70. Plunk T, Petty J, Leonhardt T. *Learn Powershell in a Month of Lunches: Covers Windows, Linux, and macOS*. Shelter Island, New York, Manning Publications, 2022, 345. ISBN: 978-1617296963.
71. Hasselbring W. Formalization of federated schema architectural style variability. *J Softw Eng Appl* 2015;**8**:72–92.
72. Gramer R. Israel changed intelligence sharing with U.S. after Trump comments to Russians. *Foreign Policy*, 24 May 2017. https://foreignpolicy.com/2017/05/24/israel-changed-intelligence-sharing-with-u-s-after-trump-comments-to-russians/ (6 July 2021, date last accessed).
73. Bater J, Elliott G, Eggen C. *et al*. SMCQL: Secure querying for federated databases. *Proc LVDB Endow* 2017;**10**:673–684. http://users.eecs.northwestern.edu/ jennie/pubs/smcql.pdf (7 April 2022, date last accessed).
74. Sallam A, Bertino E. Result-based detection of insider threats to relational databases. In *Proceedings of Ninth ACM Conference on Data and Application Security and Privacy (CODASPY '19). Association for Computing Machinery, New York, NY*, 133–14, 25–27 March 2019.
75. Berlusconi G. Come at the king, you best not miss: criminal network adaptation after law enforcement targeting of key players. *Global Crime* 2022;**23**:44–64.
76. O'Grady C. *The Price of Protecting Rhinos*. The Atlantic, 13 January 2020. https://www.theatlantic.com/science/archive/2020/01/war-rhino-poaching/604801/ (4 June 2022, date last accessed).
77. Cheng AM. The causes, impact and detection of duplicate observations. *SAS Global Forum*, 1998. https://www.lexjansen.com/pharmasug/1998/CODERS/CHENG.PDF (18 February 2022, date last accessed).
78. Just BH, Marc D, Munns M. *et al*. Why patient matching is a challenge: Research on master patient index (MPI) data discrepancies in key identifying fields. *Perspect Health Inf Manag* 2016;**13**:1e.
79. Yujian L, Bo L. A normalized Levenshtein distance metric. *IEEE Trans Pattern Anal Mach Intell* 2007;**29**:1091–5.
80. Besta M, Kanakagiri R, Mustafa H. *et al*. Communication-efficient Jaccard similarity for high-performance distributed genome comparisons. *2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, New Orleans, LA, 1122–32, 18–22 May 2020.
81. Bhattacharya I, Getoor L. Collective entity resolution in relational data. *ACM Trans Knowl Discov Data (TKDD)* 2007;**1**:5–es.
82. Haas TC, Ferreira SM. Finding politically feasible conservation strategies: the case of wildlife trafficking. *Ecol Appl* 2018;**28**:473–94.
83. Haas TC. Database software for a confederation of wildlife trafficking investigators. *Lubar School of Business, University of Wisconsin-Milwaukee*, 2022. https://sites.uwm.edu/haas/ (10 April 2022, date last accessed).
84. WWF. *Strategies for Fighting Corruption in Wildlife Conservation; A Primer*. World Wildlife Fund and TRAFFIC, 2015. https://www.traffic.org/site/assets/files/1961/wci_strategies_for_fighting_corruption_wildlife_conservation.pdf (24 May 2022, date last accessed).
85. Koehler M. Has the FCPA been successful in achieving its objectives? *Univ Ill Law Rev* 2019;**4**:1267–320.
86. Dávid-Barrett E. Business unusual: collective action against bribery in international business. *Crime Law Soc Change* 2019;**71**:151–70.
87. SELC. Conservation groups defend Cape Hatteras National Seashore. *Southern Environmental Law Center, Press Release*, 13 March 2012. https://www.southernenvironment.org/press-release/conservation-groups-defend-cape-hatteras-national-seashore/ (3 June 2022, date last accessed).
88. Nakhwal J, McGuigan K. Risky business: the use of INTERPOL by states in politically motivated cases against company executives. Financier Worldwide, 2019, 25. https://www.financierworldwide.com/risky-business-the-use-of-interpol-by-states-in-politically-motivated-cases-against-company-executives#.Yp9nEO7MK70(7 June 2022, date last accessed).
89. Meacham S. Weaponizing the police: authoritarian abuse of Interpol. *Harvard International Review*, 11 April 2022. https://hir.harvard.edu/weaponizing-the-police-authoritarian-abuse-of-interpol/ (1 June 2022, date last accessed).
90. The Economist. *Who will police Interpol?* The Economist, 4 December 2021. https://www.economist.com/leaders/2021/12/04/who-will-police-interpol (17 March 2023, date last accessed).
91. Jacobs J. *Has Interpol become the long arm of oppressive regimes?* The Guardian, 17 October 2021. https://www.theguardian.com/global-development/2021/oct/17/has-interpol-become-the-long-arm-of-oppressive-regimes (7 June 2022, date last accessed).
92. Lu M, Zhang Z, Qu Z. *et al*. LPANNI: Overlapping community detection using label propagation in large-scale complex networks. *IEEE Trans Knowl Data Eng* 2019;**31**:1736–49.
93. Li Y, Liu Y. A wrapper feature selection method based on simulated annealing algorithm for prostate protein mass spectrometry data. *IEEE Symposium on Computational Intelligence in Bioinformatics and Computational Biology, Sun Valley, ID, 2008*, 195–200, 15–17 September 2008, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4675778 (18 July 2021, date last accessed).

Appendix: optimal removal algorithm

Using the Simulated Annealing (SA) optimization algorithm [93], select at random, sets of players to remove from the simulator's WTS network—each time computing the per-year poaching rate. Stop performing these random draws when a set is found that causes the largest predicted drop in this rate. A candidate set of m players to remove is formed by randomly selecting $r < m$ "swap-in" players from the current set of m "swapped-out" players, and an equal number of "swap-out" players from the current WTS network—and then removing from the network, these r "swap-out" players, and putting back into the network these r "swap-in" players.