Title

A business that can’t lose: Investing in attacks against the Colombian power grid

Authors

Barreto, Carlos
Cardenas, Alvaro A
Holmes, Jennifer
et al.

Publication Date

2019-09-01

DOI

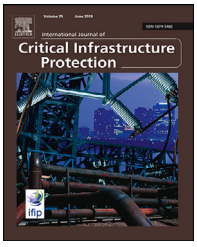
10.1016/j.ijcip.2019.05.006

Peer reviewed

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/IJCIP



A business that can't lose: Investing in attacks against the Colombian power grid

Carlos Barreto[a,*], *Alvaro A. Cardenas*[b], *Jennifer Holmes*[c], *Agustin Palao*[c], *Juan Carlos Restrepo*[d]

[a] *Department of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, Tennessee, United States*
[b] *Department of Computer Engineering, University of California, Santa Cruz, Santa Cruz, California, United States*
[c] *School of Economic, Political & Policy Sciences, University of Texas at Dallas, Richardson, Texas, United States*
[d] *Sociopolitical Risk Coordinator with INTERCOLOMBIA S.A. E.S.P., Medellín, Colombia*

ARTICLE INFO

Article history:
Received 9 December 2018
Revised 10 April 2019
Accepted 14 May 2019
Available online 31 May 2019

Keywords:
Security transmission lines
Power systems
Contracts
Economics
Game theory
Mechanism design

ABSTRACT

In 2005 a company in charge of repairing electric transmission towers made a deal with guerrilla militants to demolish the towers. This company thrived, because the attacks were attributed to guerrilla groups, who commit these attacks often. However, the number of attacks increased significantly, raising alarms and leading to the discovery of the plot. We model this situation as a game between contractors and the power transmission company, and show how misaligned incentives enabled contractors to profit by colluding with guerrilla groups. We also analyze how to modify the contractual policies reducing the incentives to collude with guerrillas. In particular, the transmission company can prevent attacks by creating competition and exploiting market inefficiencies.

1. Introduction

Colombia has suffered decades of internal conflict between the government, paramilitary groups, and leftist guerrillas. In this asymmetric conflict the rebel groups have used unconventional military strategies, such as kidnaps, extortions, and attacks against *critical infrastructures*. According to a study documenting attacks against the electricity sector worldwide, Colombia suffered 2470 attacks (out of 5846 tabulated in the study), far more than any other country [1]. The next most afflicted country in the study was Slovenia, with 810 attacks against the electric sector.

It is difficult to deal with terrorists, because they are determined adversaries who pursue political or ideological objectives that oppose the official governments. Since the parties often deny the demands of the adversary, clashes seem unavoidable. Besides, terrorists actors also pursue economic interests, which may lessen or exacerbate their actions.

Here we present a case study that shows the importance of economic incentives for the security of critical infrastructures. In this bizarre case, Electroservicios, a contractor in

* Corresponding author.
E-mail addresses: carlos.a.barreto@vanderbilt.edu (C. Barreto), alacarde@ucsc.edu (A.A. Cardenas), jholmes@utdallas.edu (J. Holmes), agustin.palaomendizabal@utdallas.edu (A. Palao), jcrestrepo@intercolombia.com (J.C. Restrepo).

https://doi.org/10.1016/j.ijcip.2019.05.006
1874-5482/

charge of repairing transmission towers, payed guerrilla militants to destroy towers that it would repair afterwards. Concretely, Electroservicios paid around $4k USD to bring down each tower, but received around $75k USD to repair them. With this corrupt plot Electroservicios managed to thrive, sponsoring around 215 attacks on electric towers during 2005–2008 [2,3].

The experience of the Colombian government and private sectors, who operate critical infrastructures under continuous attacks, can provide insights into the strategic and adversarial nature of defender-attacker conflicts. In particular, some elements of such conflicts can be relevant for cyber-security and the protection of other critical infrastructures. For example, security problems aggravated due to misaligned incentives, can occur in other industries. Concretely, Brian Krebs reported that a company specialized in protecting against distributed denial of service (DDoS) attacks co-authored the Mirai malware to attack some of its customers [4]. In this way, the company thrived by manufacturing both threats and protections, while the victims had no choice but to accept this deal.

In this paper we analyze perverse incentives that aggravate security problems and strategies to prevent them. We start by providing some background on attacks to the Colombian power grid in Section 2. The historical data shows that the number of attacks sponsored by Electroservicios exceeded considerably the usual guerrilla activity.

In Section 3 we present the bidding process used to select contractors and we show how Electroservicios profited by colluding with guerrilla groups. In particular, the perverse incentives arise because the infrastructure administrator cannot verify the identity (or the motivation) of the attackers. For example, Electroservicios was successful (at least for a while), because the authorities associated its attacks with the usual actions of guerrilla groups.

An infrastructure administrator may prevent corruption by reducing the information asymmetries, e.g., developing monitoring schemes to detect frauds. However, here we analyze how to prevent frauds by modifying the mechanism to select contractors. We find that it is possible to reduce the perverse incentives by assigning repair contracts randomly. In Section 4 we propose and analyze a random selection mechanism and illustrate its efficacy with a numerical example. We also show how audits on the repairs can mitigate the contractor's perverse incentives.

Finally, Section 5 shows that other parties involved in the repair process (e.g., local workers) may have incentives to attack the system. We also show how the mechanism from Section 4 can mitigate the perverse incentives of workers. In Section 6 we summarize related work and conclude with a discussion in Section 7.

2. Analysis of attacks against the power grid

Colombia has suffered more than five decades of conflict between leftist guerrillas, right-wing paramilitaries, government military forces, and illegal drug trade. The largest leftist guerrilla in the nation is the FARC (Fuerzas Armadas Revolucionarias de Colombia). The rebels have targeted the critical infrastructure of Colombia, such as the power grid and oil pipes, to expose government weaknesses, to force negotiations, and to create diversions for other strategic actions (Fig. 1 shows an example of a transmission tower destroyed by a guerrilla group).

Fig. 1 – Transmission tower destroyed by attack. Photo courtesy of Interconexion Electrica S.A. E.S.P. (ISA).

The attacks against the power grid can be intense and may affect large geographical areas. For example, in January 2002, the FARC attacked 38 towers, leaving 28 municipalities with outages and brownouts [5]. Also, the attacks may affect major cities. On March 2000, an attack on 11 towers and an electricity substation caused blackouts in at least seven cities, including the capital Bogotá [6]. Such attacks disrupt the economy and cause significant losses; in particular, the cost of attacks has been estimated to be 1.8% of commercial activities [7]. Besides, the attacks also endanger human lives. In 2012, five workers were killed and six others were wounded by landmines left behind to sabotage relief works in Tumaco [8].

The companies operating the power system have gained valuable experience maintaining the service provision despite constant attacks by rebels. For instance, repairing electric towers took around 13 days in 2004, while in 2009 it took 6 days on average. They also established new protocols, such as installing provisional towers whenever appropriate while the repairs finished.

The southwest region of Colombia,[1] where irregular tower attacks happened, has 2,744 towers and 17 main power lines. They represent only 18% of the total number of towers in the power grid and 20% of the total number of main power circuits. Fig. 2 shows the percentage attacks in the southwest region compared with attacks in the rest of the power grid during the 2000–2010 period. This figure shows that the number of attacks intensified in the southwest region during the 2006–2008 period.

Fig. 3 presents a comparison of the number tower attacks versus the number of violent events attributed to guerrillas. The disparity of tower attacks with respect to guerrilla violence in the southwest region of Colombia

[1] The southwest region includes the following departments: Cauca, Nariño, Valle del Cauca, Huila, and Tolima.

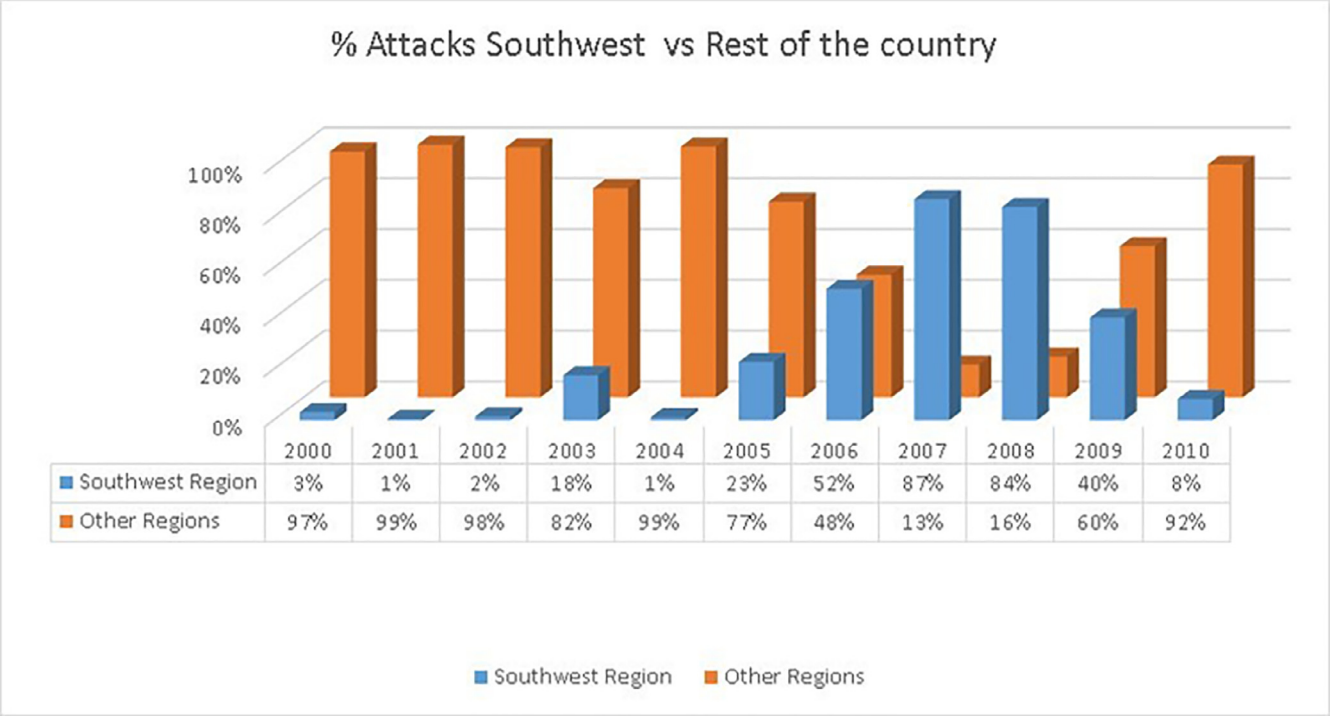


Fig. 2 – Tower attacks comparison. The attacks increase in the southwest region during 2005–2008.

Table 1 – Tower attacks - Guerrilla violence ratios 2000–2009. the highest ratios between power grid attacks compared to other types of violence are colored in red, yellow and green.

ISA TOWER ATTACKS VS. CINEP VIOLENT EVENTS

Depto_ID	Department	2000			2001			2002			2003			2004			2005			2006			2007			2008			2009			ISA Total Events
		ISA	CINEP	Ratio	ISA	CINEP	Ratio	ISA	CINEP	Ratio	ISA	CINEP	Ratio	ISA	CINEP	Ratio	ISA	CINEP	Ratio	ISA	CINEP	Ratio	ISA	CINEP	Ratio	ISA	CINEP	Ratio	ISA	CINEP	Ratio	
5	ANTIOQUIA	204	599	0.34	154	551	0.28	121	559	0.22	94	346	0.27	38	196	0.19	43	116	0.37	24	168	0.14	10	114	0.09	11	58	0.19	11	36	0.31	710
19	CAUCA	2	235	0.01	0	180	0.00	2	193	0.01	20	115	0.17	1	117	0.01	8	50	0.16	49	66	0.74	72	104	0.69	73	34	2.15	10	49	0.20	237
54	NORTE DE SANTANDER	31	153	0.20	20	224	0.09	19	206	0.09	3	103	0.03	6	58	0.10	26	49	0.53	22	69	0.32	0	39	0.00	0	37	0.00	12	59	0.20	139
13	BOLIVAR	0	184	0.00	0	148	0.00	28	126	0.22	26	104	0.25	17	68	0.25	7	76	0.09	18	44	0.41	0	72	0.00	1	21	0.05	0	19	0.00	97
81	ARAUCA	0	40	0.00	0	80	0.00	8	101	0.08	19	90	0.21	11	38	0.29	14	34	0.41	1	57	0.02	1	23	0.04	0	27	0.00	4	18	0.22	58
68	SANTANDER	26	199	0.13	12	112	0.11	7	112	0.06	2	54	0.04	0	18	0.00	0	12	0.00	0	29	0.00	0	19	0.00	0	12	0.00	0	12	0.00	47
25	CUNDINAMARCA	6	55	0.11	1	63	0.02	34	101	0.34	4	48	0.08	0	4	0.00	0	5	0.00	0	1	0.00	0	0	0.00	0	0	0.00	0	2	0.00	45
73	TOLIMA	2	108	0.02	1	125	0.01	1	134	0.01	7	88	0.08	0	90	0.00	9	59	0.15	14	44	0.32	0	143	0.00	10	88	0.11	0	46	0.00	44
76	VALLE DEL CAUCA	4	137	0.03	0	82	0.00	0	86	0.00	1	66	0.02	0	44	0.00	8	28	0.29	9	40	0.23	2	38	0.05	6	9	0.67	0	8	0.00	30
70	SUCRE	0	52	0.00	0	73	0.00	13	86	0.15	6	71	0.08	5	65	0.08	1	55	0.02	3	7	0.43	0	11	0.00	0	7	0.00	0	0	0.00	28
17	CALDAS	3	44	0.07	2	50	0.04	18	129	0.14	0	50	0.00	2	47	0.04	0	24	0.00	0	23	0.00	0	43	0.00	0	24	0.00	0	0	0.00	25
15	BOYACA	0	25	0.00	0	21	0.00	4	36	0.11	11	19	0.58	0	18	0.00	2	7	0.29	1	9	0.11	0	6	0.00	0	4	0.00	0	10	0.00	18
52	NARIÑO	1	59	0.02	0	63	0.00	1	122	0.01	3	46	0.07	0	48	0.00	3	33	0.09	1	34	0.03	0	61	0.00	0	37	0.00	9	38	0.24	18
44	LA GUAJIRA	0	17	0.00	0	55	0.00	1	42	0.02	7	18	0.39	0	17	0.00	0	19	0.00	2	33	0.06	0	21	0.00	5	8	0.63	1	5	0.20	16
41	HUILA	0	96	0.00	0	120	0.00	0	201	0.00	6	106	0.06	0	47	0.00	0	39	0.00	3	31	0.10	0	43	0.00	0	30	0.00	0	39	0.00	9
23	CORDOBA	0	14	0.00	3	31	0.10	0	28	0.00	0	8	0.00	0	15	0.00	0	12	0.00	0	7	0.00	0	11	0.00	0	14	0.00	0	14	0.00	3
8	ATLANTICO	0	3	0.00	0	1	0.00	1	8	0.13	0	2	0.00	0	3	0.00	1	4	0.25	0	3	0.00	0	0	0.00	0	1	0.00	0	1	0.00	2
66	RISARALDA	1	52	0.02	1	33	0.03	0	65	0.00	0	47	0.00	0	16	0.00	0	16	0.00	0	10	0.00	0	9	0.00	0	0	0.00	0	3	0.00	2

Ratios higher than 1
Ratios between 0.51 and 0.99
Ratios between 0.1 and 0.5

is notorious. In particular, while the number of guerrilla violence remains stable in this period (around 63 violent events on average), the number of tower attacks increased significantly.

Table 1 shows the ratio between tower attacks and guerrilla violence per department[2] (we highlight the highest ratios with color red, yellow, and green). Observe that Antioquia is consistently in the first three places, e.g., Antioquia suffered most of the attacks between 2000 and 2009 (710 attacks on towers in total). However, in the 2005–2008 period, Antioquia switched positions with other departments, especially with Cauca, which experienced a swiftly increment in the number of tower attacks. In fact, from 2006 to 2008 Cauca had the largest ratio of towers attacked vs. violent events, reaching the highest ratio in the table (by far) in 2008, with tower attacks doubling other violent actions.

After analyzing the aforementioned anomalies in Cauca, ISA (the major service provider of the Colombian power grid)

[2] We extract the activities of guerrillas from the database of actors and conflict dynamics, compiled by the CINEP (Centro de Investigación y Educación Popular).

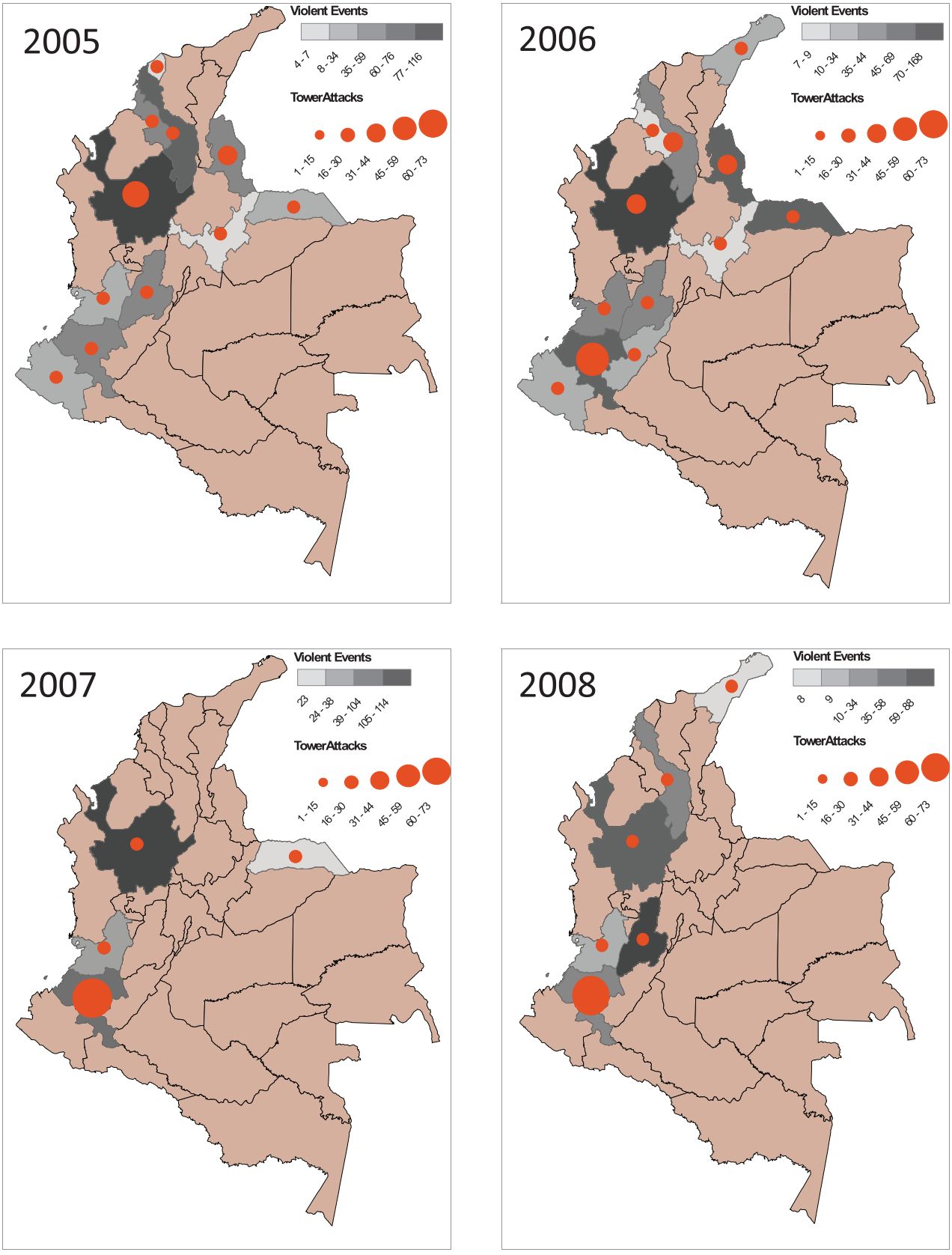


Fig. 3 – Tower attacks - Violence comparison 2005–2008.

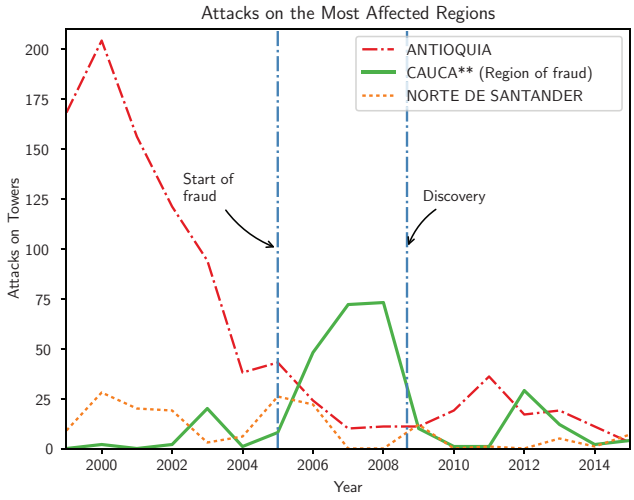


Fig. 4 – Number of attacks on the main affected regions during 1999–2015. The intervention of Electroservicios from 2005 to 2008 raised the attacks in Cauca, which surpassing other regions known for their antecedents of violence.

examined reports from repair activities and found that the attacks had the following characteristics:

- All the towers demolished belonged to them.
- The attackers' *modus operandi* was the same (e.g., they deployed the explosives in the same place).
- The same contractor (Electroservicios) repaired almost all the towers.

After tipping off the police, the authorities infiltrated the contractor and in 2008 they discovered that Electroservicio's business boomed since 2005 thanks to its cooperation with guerrilla groups. The contractor did not attack the electric towers directly; instead, it hired four guerrilla militants to demolish the towers. Electroservicios paid each militant around $1k USD and received from $25k to $75k USD to repair each tower. Fig. 4 illustrates the time line of the attacks in Cauca, compared to attacks in other affected regions.

Electroservicios and the guerrilla militants used the following criteria to choose the targets and execute the attacks:

- They chose towers with easy access to facilitate the escape of militants and the arrival of workers.
- The guerrilla militants had instructions to damage partially the towers to allow both cheap and fast repairs.
- Electroservicios ordered the attacks only on weekdays to avoid paying overtime to its employees.

Thanks to the previous precautions, Electroservicios demonstrated competence repairing towers and also thrived, because besides increasing the frequency of the services, the planned attacks also reduced repair costs. On the other hand, ISA's estimated loses during 2005–2008 amount to $8 million USD.

2.1. *Why did it take so long to detect the fraud?*

In hindsight, the singular properties of the attacks suggest a glaring fraud; however, it was difficult to determine the cause of the anomalies. On one hand, attacks on critical infrastructures are often attributed to guerrilla groups (even when they do not claim responsibility), therefore, such anomalies may not raise alarms. In fact, a prosecutor disregarded the initial denounces by ISA due to the apparent implausibility of the allegations.

On the other hand, demonstrating the implication of the contractor required extreme caution, because hasty accusations without solid evidence would fail, allowing the culprits to flee and/or manipulate evidence. Moreover, the whistleblower also faces the risk of retaliation [9].[3] In the Electroservicios case, a prosecutor eventually agreed to investigate the case, ordering infiltrations to determine the responsibility of the contractor.

3. Traditional selection of contractors

Due the large volume of attacks, transmission companies in Colombia had to hire third parties to repair transmission towers.[4] However, selecting a service provider is a non-trivial task, since both the transmission company and the contractors have conflicting interests and asymmetric information. Concretely, while transmission companies attempt to minimize their expenses, the contractors benefit with larger payments. Hence, the contractors may conceal their private information (e.g., the repair costs and/or benefits) to improve their revenues.

Below we introduce a model of the conflict between the parties and describe typical policies used to negotiate repair services. With these models we show how Electroservicios exploited the contractual policies by colluding with guerrilla groups.

3.1. *Model of agents*

Let us assume that N contractors, which conform the set $\mathcal{C} = \{1, \ldots, N\}$, offer repair services (bids). In particular, we denote the offers of all contractors with the vector $s = [s_1, \ldots, s_N]$, where the ith contractor bids $s_i \in \mathbb{R}$.

Let us consider a transmission company that commits to a mechanism $\mathcal{M} = \langle p, t \rangle$ to select the contractor (or contractors) that will repair the towers in a given region. This mechanism specifies two functions that determine the participation and the compensation of the bidders. On one hand, $p(s) = [p_1(s), \ldots, p_N(s)]$ determines the probability of selecting each contractor given the bid vector s, where $p_i(s) \in [0, 1]$ with $\sum_i p_i(s) = 1$. On the other hand, $t(s) = [t_1(s), \ldots, t_N(s)]$ determines the payment of the contractors, with $t_i(s) \in \mathbb{R}$.

[3] Retaliation may take many forms. On one hand, the whistleblower in Electroservicios case received life threats from guerrilla groups. On the other hand, Brian Krebs suffered a 620 Gbps DDoS attack (the largest at the time) because he published a story that mentioned a co-author of the Mirai botnet.

[4] The transmission companies designated a single contractor to repair the towers in a given region.

Now, let us define the profit of the agents with the mechanism $\mathcal{M}$. First, we define the expected losses of the transmission company as

$$v(s) = \theta\left(l + \sum_i p_i(s)t_i(s)\right), \tag{1}$$

where θ represents the number of towers damaged with legitimate attacks, l represents losses caused by the interruption of the electricity flow, and $\sum_i p_i(s)t_i(s)$ represents the expected repair costs.[5]

Second, we define the expected profit of each contractor $i \in \mathcal{C}$ as their expected income minus the expenses, that is,

$$u_i(s_i, s_{-i}) = \theta p_i(s)(t_i(s) - E), \tag{2}$$

where $s_{-i} = [s_j]_{j\neq i}$ represents the bids of all, except the ith contractor. On the other hand, E represents the expected expenses to repair a tower, which comprises the costs to mobilize equipment, materials, and personnel to repair a tower.[6]

Additionally, we assume that each contractor i demands some minimum return to accept a repair contract. We represent this restriction with

$$u_i(s_i, s_{-i}) \geq r_i\theta p_i(s)E, \tag{3}$$

where $\theta p_i(s)E$ represents the expected expenses for repairing θ towers and $r_i \geq 0$ represents the return of investment required by the ith contractor. Thus, the minimum bid that satisfies the return required by the contractor (see (2) and (3)) is

$$s_i^* = (1 + r_i)E. \tag{4}$$

We assume that the transmission company has limited knowledge and ignores the minimum profit r_iE required by the ith contractor. In the literature of *mechanism design*, the private information of each agent, in this case r_iE, represents the *type* of the bidders. Although in practice the transmission company can estimate the damage of each tower to adjust the payments t, we assume that the transmission company ignores the value of the repair expenses E. This is the worst case in which the transmission company makes the same payment independently of the type of attack. In other words, the transmission company cannot distinguish legitimate from sponsored attacks.

In summary, the mechanism $\mathcal{M}$ creates a game in which the contractors' profit depends on their own bids s_i and the bids of other contractors s_{-i}. The timing of the game is as follows:

i. The principal publishes a mechanism $\mathcal{M} = \langle p, t\rangle$.
ii. The contractors realize their private information and submit a message (bid) s_i to the principal.
iii. The principal determines the outcome (participation and compensation) based on the bid vector s.

3.2. *Selection of lawful contractors*

Economic theory has an extensive literature on the design of policies to reach a desired goal despite the conflicting objectives and the asymmetric information of the participants. Specifically, some celebrated results from *mechanism design* demonstrate that auctions can both elicit private information from agents and maximize the revenue of the auctioneer [10].

In this case, the transmission company can use a *reverse auction*[7] to select the best contractor. In a reverse auction the transmission company wants to buy a service (e.g., tower repair) and multiple sellers (who must satisfy the contract specifications) offer bids on the contract (e.g., repair costs). The reverse auction can have many stages in which bidders make offers using closed envelopes. The bids at each stage start at the lowest bid offered in the previous stage; thus, the sellers compete reducing their bids and the seller with the lower bid wins the contract.

Let us illustrate why a reverse auction elicits private information from the contractors and maximizes the revenue of the transmission company. On one hand, in a reverse auction each contractor (if selected) may receive a compensation equal to its bid, that is,

$$t_i(s) = s_i. \tag{5}$$

Moreover, the transmission company may select the probability vector p to minimize the costs (see (1)); hence, p solves

$$\begin{aligned} \underset{p_1,\ldots,p_N}{\text{minimize}} \quad & \theta\left(l + \sum_i p_i t_i(s)\right) = \theta\left(l + \sum_i p_i s_i\right) \\ \text{subject to} \quad & \sum_i p_i = 1, \\ & p_i \geq 0. \end{aligned}$$

Although we formulate the mechanism allowing random selection, the optimal selection rule, denoted p^d, is deterministic and satisfies

$$p_i^d = \begin{cases} 1 & \text{if } s_i \leq s_j \quad i \neq j \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

In other words, the transmission company minimizes its costs by selecting the contractor that offers the minimum bid.[8]

On the other hand, a mechanism given by (5) and (6) incentives contractors to offer the minimum cost that they can

[5] Although the Colombian regulations do not penalize failures to deliver electricity caused by terrorist attacks, transmission companies still must purchase more expensive sources of electricity (if available), such as carbon-based fuels.

[6] Although the losses l and the repair expenses E may vary in each attack, we assume that the transmission company and the contractors use average values to determine their strategies.

[7] Auctions are mechanisms that allow a seller to elicit the private information from buyers and assign a good to the buyer willing to pay the largest quantity [11]. A reverse auction follows the same principle, but inverting the roles of the parties. According to the Colombian contracting code of public administrations [12,13], public biddings must follow reverse auctions.

[8] In Section 4 we show that random selection of bidders contributes to prevent attacks.

accept, denoted s_i^*. In particular, with enough competition, selecting $s_i = s_i^*$ is a *Nash Equilibrium*, that is, when other participants make their minimum bid (denoted s_{-i}^*), the ith contractor weakly prefers to to bid s_i^* over other strategy s_i, that is,

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*).$$

Observe that if the contractor offers a bid $s_i = s_i^* + \epsilon$, with $\epsilon > 0$, then the contractor may lose the bid (even if the contractor can offer the lowest bid). On the other hand, a bid $s_i = s_i^* - \epsilon$ violates the restriction in (4), therefore, the contractor may not receive its minimum expected compensation.

In summary, the auction mechanism, denoted $\mathcal{M}_d = \langle p^d, t \rangle$, incentives contractors to reveal their private information, which allows the transmission company minimize its expenses. Observe that the auction assumes implicitly that no agent can control the repair expenses E; however, this assumption fails when the contractors secretly cooperate with guerrilla militants. Below we show how the bidding strategy changes considering collusions with guerrilla groups.

3.3. *Modeling the Electroservicios case*

A contractor that colludes with guerrilla militants augments its action space, because now it decides whether to sponsor attacks. Let the vector $a = [a_1, \ldots, a_N]$ be the attack strategy of all contractors, with $a_i \in \mathbb{R}_{\geq 0}$ for $i \in \mathcal{C}$.

We define the profit associated to sponsored attacks as

$$w_i(s, a) = p_i(s)(s_i - E_a) \sum_j a_j - b(a_i), \tag{7}$$

where E_a is the cost to repair a tower damaged with a sponsored attack. Since carefully planned (sponsored) attacks reduce the repair expenses, then $E_a < E$. This implies that the contractor earns a larger profit with sponsored attacks, compared with legitimate attacks.

On the other hand, the function $b(a_i)$ represents the bribe or cost to launch a_i attacks. We assume that the bribe $b : \mathbb{R}_{\geq 0} \to \mathbb{R}_+$ is convex and strictly increases with the number the attacks, because 1) the risk of being captured increases with the frequency of the attacks (since the military forces would increase the frequency of patrols); and 2) the guerrillas may charge the opportunity cost incurred attacking electric towers rather than doing other activities. Hence, we assume that the bribe function $b(\cdot)$ satisfies $\dot{b} > 0$ and $\ddot{b} \geq 0$.

Remark 1. We ignore the risk of detection for the contractor, because in the worst case the transmission company won't distinguish sponsored from legitimate guerrilla attacks.

The mechanism $\mathcal{M}_d$ selects only one contractor to repair the towers within a region. Hence the contractor who wins the auction also repairs all the towers affected with sponsored attacks, which amount to $\Sigma_j a_j$. In addition, given the timing of the game, the decision to sponsor attacks takes place once the auction finishes. As a consequence, only the contractors who wins the auction may have incentives to sponsor attacks. Thus, we can assume that if the ith contractor wins the auction, then $a_j = 0$ for $j \neq i$, $\sum_j a_j = a_i$. Hence, (9) becomes

$$w_i(s, a_i) = a_i(s_i - E_a) - b(a_i). \tag{8}$$

In summary, the total profit of a contractor will have two components, given by both the legitimate (see (2)) and the sponsored attacks (see (8)). Consequently, a contractor can offer lower bids anticipating the benefit of sponsoring attacks. In particular, the bid s and attack a that guarantee the minimum return required by the contractors satisfy

$$u_i(s) + w_i(s, a) \geq r_i p_i(s)(\theta E + a_i E_a + b(a_i)), \tag{9}$$

where $\theta E + a_i E_a + b(a_i)$ represent the total expenses for sponsoring attacks. Thus, the minimum bid that a contractor can offer, denoted $s_i^a(a_i)$, satisfies (9) with equality

$$s_i^a(a_i) = s_i^* + (1 + r_i)\frac{b(a_i) - (E - E_a)a_i}{\theta + a_i}. \tag{10}$$

Observe that when $a = 0$ the contractor cannot offer lower bids, that is, $s_i^a(0) = s_i^*$; however, a contractor can reduce the bids (i.e., $s_i^a(a_i) < s_i^*$) if the benefit from sponsored attacks $(E - E_a)a_i$ exceeds the cost of the attacks $b(a_i)$. Nevertheless, this reduces the profit of the contractor.

In the next example we reconstruct the case of Electroservicios using information from news reports and assuming worst case scenarios. We show that the failure to estimate the real expenses (E and E_a) play a vital role for the success of the attack. Also, we illustrate how lower bids impact the profit of the corrupt contractor.

3.4. *Numerical example*

3.4.1. *Recreating the Electroservicios case*

Here we assume that the contractor does not offer reduced bids; therefore, it can collect the maximum profit from the sponsored attacks. In other words, the contractor bids $s_i = s_i^*$, which satisfies (4).

The news reports mention that ISA (the transmission company) paid from \$75k to \$25k USD to repair electricity towers [2]. For simplicity, we consider that legitimate attacks cause maximum damage, while sponsored attacks do the opposite, reducing the expenses to the minimum. Hence, we assume that $t_{max} = \$75k$ and $t_{min} = \$25k$ USD are fair compensations for repairing towers damaged by legitimate and sponsored attacks, respectively.

According to the previous considerations we define the usual payment for repair services as

$$t_i = s_i^* = t_{max},$$

where the ith agent is the winner of the auction.

With a rate of return $r_i = 10\%$, we can use (4) to find the expenses to repair each tower (which suffered a legitimate attack)

$$E = \frac{t_{max}}{(1 + r_i)} = \$68,182.$$

In a similar way, we define the expenses to repair towers that suffered sponsored attacks as

$$E_a = \frac{t_{min}}{(1+r_i)} = \$22{,}272.$$

From the reports we know that the contractor payed around \$4k USD to attack each tower. Although the reports give little information about the form of the bribe function $b(\cdot)$, we follow the standard practices in economics and assume that this function is increasing convex. In particular, we define the bribe function as in [14]

$$b(a_i) = a_i b_0 + \lambda \frac{(1+\alpha)^{a_i} - 1}{\alpha}. \tag{11}$$

Let us assume that the bribe required to attack one tower as $b(1) = b_0 + \lambda = \$4$k USD, where b_0 represents the fixed cost and $\lambda = 0.2b_0$ is a parameter of the variable cost (see (11)). Consequently, $b(1) = 1.2b_0$ and $b_0 = \$3,333$. Furthermore, we choose α to satisfy the following assumptions about the optimal number of attacks.

The story by Caracol [3] reports that Electroservicios sponsored approximately 215 attacks on energy towers during 3 years. Here we assume that the number of sponsored attacks was optimal, that is, the contractor had maximum profit with $a_i^* = 215/3 \approx 72$ attacks per year. In consequence, a_i^* must satisfy (8), that is,

$$a_i^* \in \arg\max_{a_i} a_i(s_i^* - E_a) - b(a_i).$$

We find numerically that the previous expression is true with $\alpha = 0.0625$. Finally, we estimate the number of legitimate attacks as $\theta = 20$.

3.4.2. *Role of asymmetric information*

Now we show how asymmetric information creates incentives to sponsor attacks. Let us represent with $\hat{t}(\gamma) = \gamma t_{min} + (1-\gamma)t_{max}$ an estimation of the costs to repair towers targeted by sponsored attacks. Here $\gamma \in [0, 1]$ represents the accuracy of the estimation. Thus, estimations with minimum accuracy ($\gamma = 0$) will lead to the maximum payment $\hat{t}(0) = t_{max}$, while accurate estimations ($\gamma = 1$) will lead to the appropriate payment, in this case, $\hat{t}(1) = t_{min}$.

Let us define the profit of sponsored attacks (see (8)) as a function of the estimation accuracy γ

$$w_i(s, a_i, \gamma) = a_i(\hat{t}(\gamma) - E_a) - b(a_i). \tag{12}$$

Fig. 5 shows the optimal number of attacks a_i^* that maximizes the contractor's profit in (12) as a function γ. In this case, the contractor reduces the number of sponsored attacks as the cost's estimations become more accurate. In particular, ignoring the minimum rate of return, sponsored attacks become unprofitable if $\hat{t}(\gamma) - E_a < b(1)$, for some $\gamma \in [0, 1]$.

3.4.3. *Contractor's bidding strategies*

Fig. 6 shows the profit of a contractor when it uses two different bids, namely the optimal bid without attacks s_i^* (see from (4)) and the minimum bid with a_i planned attacks $s_{min}(a_i)$ (see (10)). In this case the contractor can offer more competitive bids at the expenses of a lower profit; however, the contractor still has incentives to sponsor attacks.

4. Designing contracts to prevent attacks

In this section we discuss alternatives to prevent attacks and introduce a modified auction that discourage sponsored attacks. The new auction introduces a competition among contractors and leverages market inefficiencies (such as the *tragedy of the commons* [15] or the *price of anarchy* [16]) to reduce the total number of attacks.

4.1. *Strategies to prevent attacks*

The transmission company can prevent attacks by reducing the asymmetries in information. For example, direct monitoring, such as the investigations that revealed the fraud, can expose corrupt companies, but are prohibitively expensive. Moreover, indirect monitoring, such as Yardstick competition, helps identifying anomalous behaviors by comparing the bids of similar firms [17]. Although such mechanism help to identify anomalous small bids, a malicious contractor can anticipate the detection efforts and offer bids that avoid alarms.

The principal[9] may redesign the mechanism to guarantee that the participants report their private information, e.g., the real cost of repairs and/or the capacity to collude with guerrillas. Such mechanism should incentive contractors to report vulnerabilities in the contracts, just as bug bounty programs incentive individuals to report software vulnerabilities. In other words, the mechanism proposes a negotiation between the parties, including the guerrilla groups. We don't explore this scenario because companies that negotiate with guerrillas may face severe penalties, since economic transactions can be interpreted as cooperation with insurgents.

A third alternative consists in selecting another type of auction to assign the repair contracts. In this case, we use the celebrated *revenue equivalence theorem* (RET) to determine whether a different auction leads to the same results [10,18]. According to the RET, auctions that satisfy the following conditions yield the same expected welfare to both the principal and the bidders:[10] 1) the highest bidder wins the auction and 2) bidders with the lowest valuation expect zero surplus.

The RET is relevant because the transmission company uses an *ascending* auction to select repair services (see Section 3). Therefore, the RET implies that *first price, second price*, and *all-pay* auctions (among others) are equivalent, because the outcome (expected welfare of the participants) will be the same. That is, auctions that comply with the RET may give the contractors the same incentives to sponsor attacks. Below, we leverage the RET to design an auction that leads to a different outcome, which disincentive attacks.

[9] In the literature of mechanism design the principal is the agent that design the mechanism. Here, the principal is the transmission company.

[10] The theorem applies if the participants are risk neutral and have i.i.d. valuations.

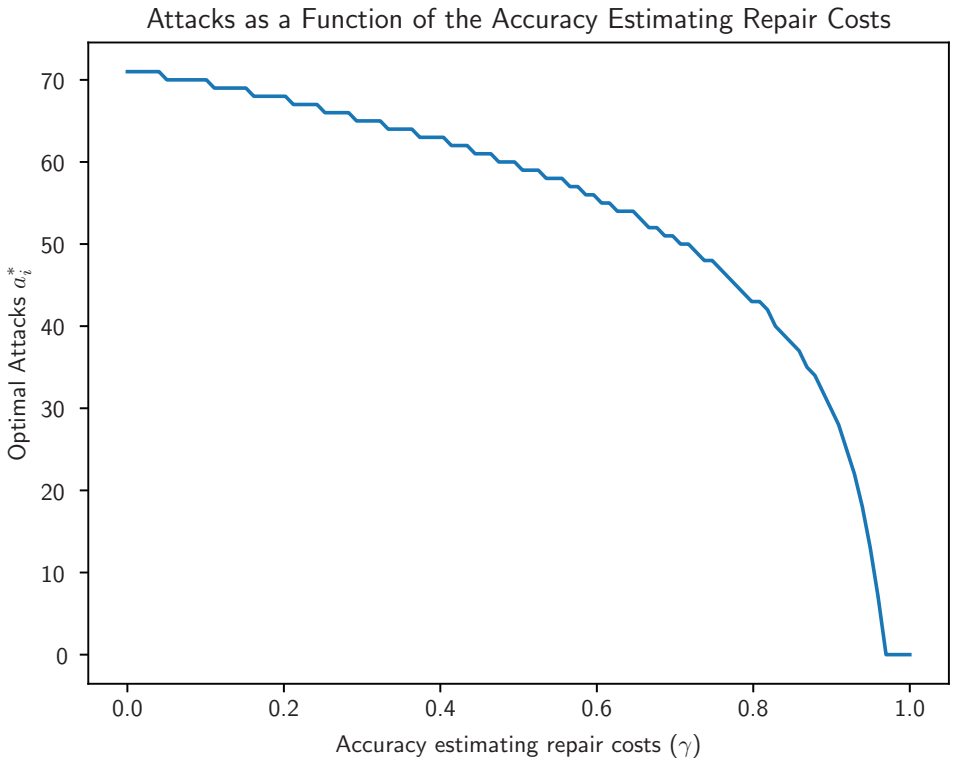


Fig. 5 – Optimal number of attacks as a function of the accuracy estimating the repair costs (γ). In this case high accuracy estimating the costs may even prevent sponsored attacks.

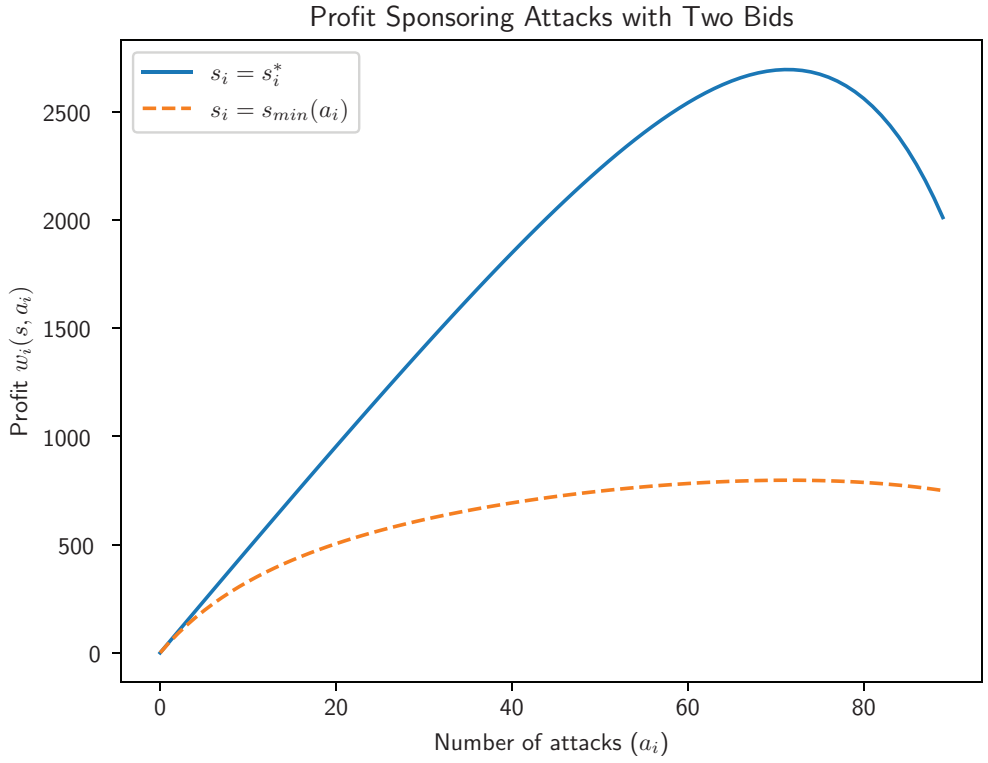


Fig. 6 – Profit of sponsored attacks $w_i(s, a)$ with two bids, namely the optimal bid without attacks s_i^* and the minimum bid allowed by sponsoring attacks $s_{min}(a_i)$. Although the contractor reduces its profit offering lower bids, sponsoring attacks is still profitable.

In this case, we propose a new mechanism $\mathcal{M}_r = \langle p^r, t \rangle$, whose selection rule p^r designates multiple contractors to repair towers within a region, rather than a single one.[11] In particular, the principal can change the game in substantial ways by selecting randomly a contractor to repair each damaged tower. On one hand, the results of the RET do not apply to $\mathcal{M}_r$, because it designates multiple contractors. As a consequence, this mechanism can change the expected welfare of the bidders. On the other hand, the timing of the game changes, because now the principal selects the contractors *ex-post*, that is, after the attacks take place.

4.2. *Random selection mechanism*

Let us assume that the principal selects a pool of n firms that can provide repair services. Without loss of generality, we define the pool as $\mathcal{C}_r = \{1 \dots, n\}$. The proposed selection mechanism change the strategy of contractors in two fundamental ways. First, any contractor from the pool, which have a positive probability of repairing each tower, may have incentives to sponsor attacks. Second, the contractors may have less incentives to sponsor attacks, with respect to the mechanism $\mathcal{M}_d$, because now a lottery determines whether they will enjoy the benefits. Here the timing is critical, because unlike $\mathcal{M}_d$, sponsoring an attack doesn't guarantee benefits.

We assume that the mechanism $\mathcal{M}_r$ creates interdependencies between the contractors, because their combined strategies may affect the cost of attacks (e.g., if they hire the same militants to attack the towers). We model this situation with a *Cournot competition*, in which the contractors compete on the number of attacks that they select. Hence, we see the guerrilla as a service provider with cost function $b(\cdot)$.

If the guerrilla is *price taker*,[12] then it is optimal for them to set prices as the marginal costs, i.e., $\dot{b}(\cdot)$. Thus, the profit from attacks (see (7)) becomes

$$w_i(s, a) = p_i^r(s)(s_i - E_a) \sum_{j \in \mathcal{C}_r} a_j - a_i \dot{b}\left(\sum_{j \in \mathcal{C}_r} a_j \right). \tag{13}$$

4.3. *Properties of the mechanism $\mathcal{M}_r$*

The contractors experience the *tragedy of the commons* with $\mathcal{M}_r$, because the self-interest reduces the collective welfare. This happens because the contractors have less incentives to sponsor attacks. Therefore, the competition between contractors improve the security of the system. We summarize this result in the following theorem.[13]

Theorem 1. *Consider the the mechanism $\mathcal{M}_r$ and a bid s such that $p_i^r(s) \in [0, 1)$ for $i \in \mathcal{C}_r$. Let a^{ne} be the Nash Equilibrium of the Cournot competition between contractors and a^{op} be their optimal collective strategy. If the bribe function satisfies $\dot{b}(z) > 0$ for $z \geq 0$, then the contractors implement strictly less attacks in the Nash Equilibrium. That is, $\sum_i a_i^{ne} < \sum_i a_i^{op}$.*

The previous results is true as long as $p_i^r(s) \in [0, 1)$, which is true if and only if the mechanism selects multiple firms.

The next result shows that, even if the contractors collude, the mechanism $\mathcal{M}_r$ guarantees that the aggregate attacks does not exceed the attacks that a single contractor would sponsor. In particular, if the transmission company selects a single contractor with bid $\tilde{s} = \sum_i p_i^r(s) s_i$ (the expected bid given p^r and s), then this contractor would sponsor $\tilde{a} = \sum_i a_i^{op}$ attacks. In other words, in the worst case the contractors may implement roughly the same number of attacks as a single contractor.

Proposition 1. *Consider a mechanism $\mathcal{M}_r$ that selects among n bidders given a bid vector s. Let a^{op} be the optimal collective strategy and a^{ne} be the Nash equilibrium when the mechanism selects a single contractor with bid $\tilde{s}_i$. If $\tilde{s}_i = \sum_i p_i^r(s) s_i$, then, $\sum_i a_i^{op} = \sum_i a_i^{ne}$.*

The previous result shows that the new contracts would fail if a large set of contractors collude in attacks, but as far as we are aware, that level of corruption hasn't been encountered in Colombia.

Now we are interested in the design of the selection rule p^r to reduce the number of attacks. The next result shows that the total number of attacks decrease with n if the expected benefit with each repair $p_i^r(s)(s_i - E_a)$ (see (13)) decreases with the size of the pool n.

Theorem 2. *Consider the mechanism $\mathcal{M}_r$ and a bid s. Let a^{ne} be the Nash Equilibrium of the Cournot competition between contractors. If*

$$\lim_{n \to \infty} p_i^r(s)(s_i - E_a) = 0 \tag{14}$$

for all i, then $\sum_i a_i^{ne} \to 0$ as $n \to \infty$.

Observe that p^r modifies the expected benefit of each repair, $p_i^r(s)(s_i - E_a)$, which in turn determines the number of attacks. Hence, the principal may design p^r to reduce the marginal valuation of all the participants. In particular, the principal can reduce the number of attacks guaranteeing that the contractors have the same expected profit, which implies that they use the same strategy. The following result specifies the properties of p^r to minimize the number of attacks given some n.

Proposition 2. *Consider the mechanism $\mathcal{M}_r$ and a bid s. If the selection probability p^r guarantees $p_i^r(s_i - E_a) = p_j^r(s_j - E_a)$ for every bidder i, j, then the the Nash equilibrium has minimum aggregated attacks.*

Remark 2. The optimal policy from Proposition 2 requires knowledge of the real expenses E_a; however, the principal may ignore such information. Therefore, the principal may use an alternative policy

$$p_i^r(s) = \frac{1}{n},$$

which satisfies (2).

[11] In fact, ISA, the transmission company, adopted a similar mechanism after the case of Electroservicios came to light.

[12] A price taker does not have power to set prices. This may be the case, because multiple insurgent groups can provide the same service (i.e., attack towers).

[13] We include the proof of this and the following results in the Appendix.

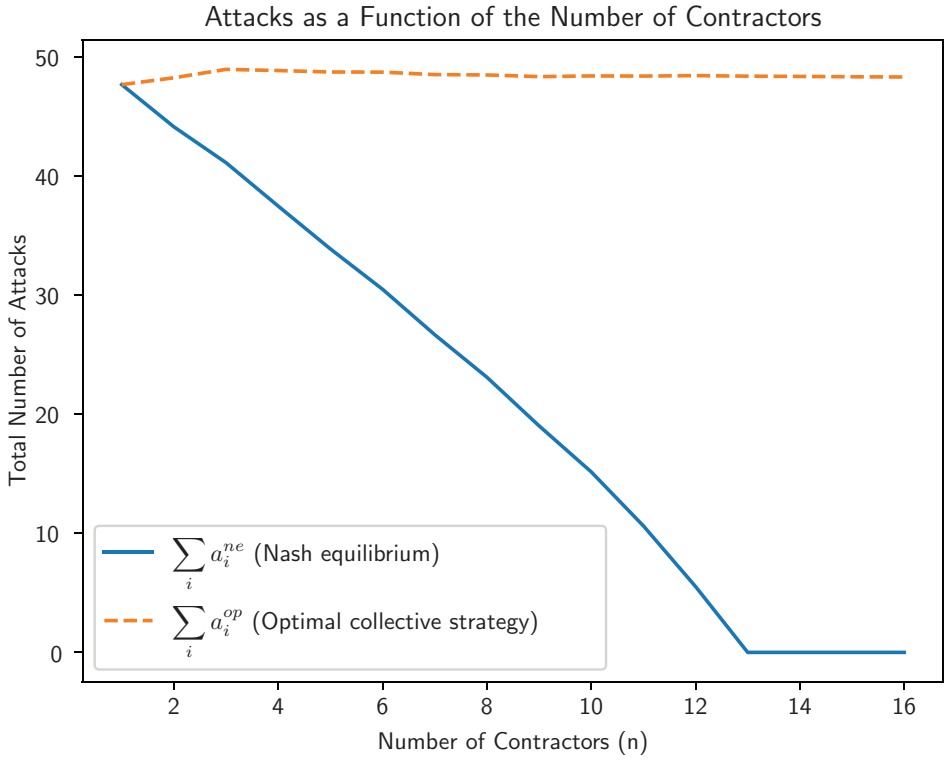


Fig. 7 – Total attacks as a function of n, the size of the pool of contractors used in $\mathcal{M}_r$. The optimal strategy for the contractors as a coalition, a^{op}, maintains the total number of attacks almost constant. However, the competition among bidders reduce the number of attacks, making them unfeasible for $n \geq 13$.

4.4. *Impact of audits*

A weakness of the mechanism lies in its dependence with the number of companies n. Here we investigate how audits can reduce information asymmetries, and in turn, mitigate the perverse incentives to sponsor attacks. Concretely, we consider audits, conducted with probability β, that reveal the real repair costs; thus, the transmission company distinguishes legitimate and sponsored attacks with probability β. Moreover, we assume that the transmission company adjusts its payment to guarantee a fair rate of return (i.e., $(1 + r_i)E_a$); hence, the corrupt contractor's net profit becomes

$$\pi_i = \begin{cases} r_i E_a, & \text{with probability } \beta \\ s_i - E_a, & \text{with probability } 1 - \beta \end{cases} \tag{15}$$

The audit modifies the expected profit of the contractors (see (13)) as follows

$$\tilde{w}_i(s, a) = p_i^r(s)\mathrm{E}[\pi_i] \sum_{j \in \mathcal{C}_r} a_j - a_i \dot{b}\left(\sum_{j \in \mathcal{C}_r} a_j\right). \tag{16}$$

The next result shows that the audit's probability β that prevents attacks decreases linearly with the number of contractors n, when $p_i^r(s) = 1/n$.

Proposition 3. *Consider the mechanism $\mathcal{M}_r$ with $p_i^r(s) = 1/n$ and an audit with probability β (see (15)). Then, the Nash equilibrium satisfies $a_i = 0$ if*

$$\beta \geq \frac{s_i - E_a - n\dot{b}(0)}{s_i - (1 + r_i)E_a}$$

for all $i \in \mathcal{C}_r$.

Fig. 7 shows an example of the total attacks as a function of n, the number of contractors that participate in the selection process. In this case we assume that each contractor bids $s_i = s_i^* = (1 + r_i)E$. We allow different bids by drawing r_i from a normal distribution with mean 0.1 and standard deviation 0.01. Furthermore, we select p^r satisfying Proposition 2.

In the worst case, when the contractors collude, the total attacks $\sum_i a_i^{opt}$ remain roughly constant; however, the competition among bidders reduce the number of attacks. Therefore, the competition created by $\mathcal{M}_r$ improves the security of the system by leveraging the tragedy of the commons, as indicated by (1). Moreover, the attacks become unfeasible if $n \geq 13$, which occurs because p^r satisfies (2).

5. Worker's incentives to sponsor attacks

The contractors often hire non-specialized workforce from the region of the accident to reduce costs. A concern is that these workers would demolish the towers to have an employment opportunity. In particular, individuals who are unemployed or have a low salary may profit by sponsoring attacks. In this section we analyze the conditions in which workers can sponsor

attacks and we use ideas from the previous section to make these attacks unprofitable.

5.1. Incentives of workers

Here we consider the conditions that make attacks profitable for a single worker. Let S be the salary paid by the repair company, S_{min} the minimum salary (either the worker's current salary or the minimum salary accepted), and τ the time that takes to repair a tower. We assume that repairing towers gives higher compensations ($S \geq S_{min}$), because it is a risky activity. Specifically, workers are exposed to bombs hidden close to the towers and they can be kidnapped by the guerrilla groups [19].

For a worker, sponsoring attacks on δ towers is profitable if the profit with an attack is higher than its cost. We can express this condition as

$$(S - S_{min})\tau\delta > b(\delta),$$

which can be rewritten as

$$S - S_{min} \geq \frac{b(\delta)}{\tau\delta}.$$

From this expression we can see that longer repair periods increase the interest in sponsoring attacks. From technical reports we know that repairs can take $\tau = 13$ days in the worst case. Consequently, at least one attack is profitable if

$$S - S_{min} \geq \frac{b(1)}{13} = \$307.7.$$

The minimum daily wage in Colombia during 2005 was $S_{min} = \$7.89$. Hence, an individual worker can sponsor an attack if his payment exceeds in at least 38 times the minimal wage ($S > 38S_{min}$), which seems unlikely. On the other hand, if the company hires m workers, they can form coalitions to share the cost of launching an attack. In such case, the workers may sponsor attacks if their individual compensation is positive, that is,

$$S - S_{min} \geq \frac{b(\delta)}{m\tau\delta}.$$

We know that, in the worst case, a tower requires 4 quadrilles (or teams) to repair it. Each quadrille is composed by 25 persons, of which 14 are specialists. Hence, we assume that 11 persons per quadrille can be hired from the local region. Consequently, we assume that the company hires $m = 44$ local workers. With these parameters we calculate the minimum salary that incentives at least one attack

$$S - S_{min} \geq \frac{b(1)}{44 \cdot 13} = \$6.98.$$

Note that in the worst case, unemployed workers have $S_{min} = 0$. Since contracts cannot offer salaries lower than the minimal wage, then a coalition of workers can get some profit sponsoring an attack, because the minimal wage ($7.89) exceeds the minimum salary $6.98 required to sponsor an attack.

The transmission company may attempt to avoid attacks selecting the salary as $S = S_{min}$. However, this approach can fail, because a low salary may not compensate honest workers for the risk that they take repairing towers.

5.2. Incentives with random selection of workers

Alternatively, we can think in a raffle to choose workers. Let us assume that the total number of possible workers is M. If m workers plot an attack expecting to be hired by the company, k workers of the coalition have the following probability of being hired:

$$B(M, m, k) = \frac{\binom{m}{k}\binom{M-m}{m-k}}{\binom{M}{m}}.$$

Therefore, the expected number of workers that belong to the coalition is

$$\bar{m} = \sum_{k=0}^{m} B(M, m, k)k < m.$$

Furthermore, $\bar{m}$ decreases as M increases. Thus, the condition for a profitable attack becomes

$$S - S_{min} \geq \frac{b(\delta)}{\tau\delta\bar{m}} > \frac{b(\delta)}{\tau\delta m}.$$

Therefore, random selection of workers hinder attempts to coordinate attacks, because the profit of workers decrease with the total number of workers M.

6. Related work

The interest for the security for critical infrastructures has grown in the last years, in part due to threats manifested in cyber attacks against Uranium enrichment plants [20], the power grid [21], and other industrial plants [22]. A weakness of critical infrastructures comes from the large number of vulnerable field devices, which extend the attack surface and may allow sophisticated attacks [23–25].

The research on cyber security often contemplates a variety of financially motivated attacks. For instance, Liu et al. [26–29] introduce attacks on devices or communication channels that can change the electricity's market equilibrium benefiting the adversary. On the other hand, the defenses often focus on designing and/or deploying mechanisms to prevent, detect, and mitigate attacks [30–34].

Moreover, the works in the literature usually analyze conflicts between two parties, namely the adversary and the defender. However, we consider a third party that colludes with the adversary and manages to profit while remaining anonymous. Such situation can occur in some cyber attacks, because it is difficult to identify the adversaries, who can do business with the defender (e.g., in cases of insider threats). Moreover, as happens in other financially motivated attacks, we propose a mechanism that mitigates the interest of the adversary.

7. Discussion and conclusions

In this paper we model a series of attacks that happened in the Colombian power system, and the actions the electric transmission company took to minimize future contractors and

Table 2 – Firms and workers operate in different ways, because they interact in different ways. Nevertheless, the random selection mechanism can reduce their perverse incentives.

	Relation	Perverse Incentives	Mechanism's impact
Firms	Compete through bids	Auction's winner colludes with guerrillas	Changes the contract's timing and creates competition
Workers	Independent	Cooperate to create labor's demand	

workers from launching similar attacks (see Table 2). This real-world example shows how economic incentives can have a dual role in the protection of a system. On one hand, misaligned incentives can be exploited by adversaries, and on the other hand, the system can be made more resilient to attacks by properly designing contracts.

Practical implementations of the proposed approach may face some issues. On one hand, the mechanism needs a large pool of contractors and workers to reduce the perverse incentives; however, in practice few firms may offer repair services. Nonetheless, audits can lessen these difficulties, because they reduce information asymmetries exploited by corrupt contractors. On the other hand, these mechanisms may result in additional transportation costs and delays, which may raise the repair expenses.

In practice, the electricity company adopted audits before choosing a repair company. Concretely, the electricity company first sends an engineer (by helicopter or by ground if possible) to estimate the damages and resources necessary for repairing the towers. They then select an appropriate contractor; however, the repair costs are based on the contracts signed with the firms.

We believe that the lessons from this case of perverse incentives can help to protect other systems against physical and cyber-attacks. For instance, Krebs [4] exposed cyber security service providers that orchestrated attacks against its clients to profit. Our scenario has some resemblances with the case in [4], because the adversaries implemented low cost attacks and operated anonymously. In such situations, random selection of firms and audits can reduce the adversary's opportunities to profit. Moreover, the random selection of workers may help to reduce the insider threat in other organizations.

Conflict of interest

The authors do not have conflict of interests that could influence this work. The financial support is properly acknowledged in the manuscript.

Acknowledgments

The authors are grateful with the anonymous reviewers, whose suggestions helped to improve the manuscript. This material is based upon work supported by NSF CMMI 1541199 and NSF CMMI 1925524 as well as by a grant from the Texas National Security Network.

Appendix

Let us introduce some preliminary definitions used in the proofs. If a^{ne} is the Nash equilibrium of the game generated by $\mathcal{M}_r$, then the strategy of the ith contractor in the Nash equilibrium solves

$$\begin{aligned} \underset{a_i}{\text{maximize}} \quad & w_i(s, a_i, a^{ne}_{-i}) \\ \text{subject to} \quad & a_i \geq 0. \end{aligned} \tag{17}$$

Let us define the Lagrangian of (17) as

$$\mathcal{L}_i(a_i, \lambda_i) = w_i(s, a_i, a^{ne}_{-i}) + \lambda_i a_i.$$

Therefore, the optimal strategy of the ith contractor satisfies the following

$$\frac{\partial}{\partial a_i}\mathcal{L}_i(a_i, \lambda_i)\Big|_{a_i = a^{ne}_i} = p^r_i(s)(s_i - E_a) - \dot{b}\left(\sum_j a^{ne}_j\right) - a^{ne}_i \ddot{b}\left(\sum_j a^{ne}_j\right) + \lambda_i = 0, \tag{18}$$

with $\lambda_i \geq 0$ and $\lambda_i a^{ne}_i = 0$. Hence, if $a^{ne}_i > 0$, then $\lambda_i = 0$.

In a similar way, the collective attack strategy that maximizes the profit of all contractors (a^{op}) satisfies

$$\frac{\partial}{\partial a_i}\sum_i w_i(s, a)\Big|_{a = a^{op}} = \sum_i p^r_i(s)(s_i - E_a) - \dot{b}\left(\sum_j a^{op}_j\right) - \sum_j a^{op}_j \ddot{b}\left(\sum_j a^{op}_j\right) + \mu_i = 0, \tag{19}$$

with $\mu_i \geq 0$ and $\mu_i a^{op}_i = 0$.

Proof of Theorem 1. We use (18) and (19) to extract the following expression

$$\frac{\partial}{\partial a_i}\sum_i w_i(s, a) = \sum_i \frac{\partial}{\partial a_i} w_i(s, a) + (n-1)\dot{b}\left(\sum_j a_j\right).$$

Now, we evaluate the previous expression in a^{ne} (we assume that $a^{ne}_i > 0$, which is the case of interest), resulting

$$\frac{\partial}{\partial a_i}\sum_i w_i(s, a)\Big|_{a = a^{ne}} = (n-1)\dot{b}\left(\sum_j a^{ne}_j\right).$$

If $n > 1$, satisfied if $p_i^r(s) \in [0, 1)$ for all $i \in \mathcal{C}$, and $\dot{b}(z) > 0$ for $z \geq 0$, then

$$\frac{\partial}{\partial a_i} \sum_i w_i(s, a)\Big|_{a=a^{ne}} > 0,$$

which implies that in the Nash equilibrium, the contractors as a collective have incentives to increase the number of attacks, that is, $a_i^{ne} < a_i^{op}$. □

Proof of Proposition 1. Let us assume that $\sum_j a_j^{op} > 0$; hence, the collective attack strategy that maximizes the profit of all contractors (a^{op}) satisfies

$$\frac{\partial}{\partial a_i} \sum_i w_i(s, a)\Big|_{a=a^{op}} = \sum_i p_i^r(s)s_i - E_a - \dot{b}\left(\sum_j a_j^{op}\right) - \sum_j a_j^{op}\ddot{b}\left(\sum_j a_j^{op}\right) = 0. \quad (20)$$

On the other hand, if the mechanism selects a single contractor with bid $\tilde{s}_i$, then it's optimal strategy a_i^{ne} satisfies

$$\frac{\partial}{\partial a_i} w_i(s, a)\Big|_{a_i=a_i^{ne}} = \tilde{s}_i - E_a - \dot{b}(a_i^{ne}) - a_i^{ne}\ddot{b}(a_i^{ne}) = 0. \quad (21)$$

Observe that (20) and (21) have the same form if $\tilde{s}_i = \sum_i p_i^r(s)s_i$. In such case, it is necessary that $\sum_j a_j^{op} = a_i^{ne}$. □

Proof of Theorem 2. If $p_i^r(s)(s_i - E_a) \to 0$ as $n \to \infty$, then for large n, the equilibrium condition in (18) holds only if $\lambda_i > 0$ (recall that $\dot{b} > 0$ and $\ddot{b} \geq 0$) This implies that $a_i^{ne} \to 0$ as $n \to \infty$. Moreover, if (14) holds for every contractor, then $\sum_i a_i^{ne} \to 0$ as we increase the size of the pool n. □

Proof of Proposition 2. First, we show that the selection probability p^r satisfies Theorem 2, that is, it reduces the attacks as n increases. Afterwards, we show that p^r minimizes the number of attacks for a given n.

Let $p_i^r(s_i - E_a) = \sigma_n$ for all i; hence,

$$\sum_{i=1}^{n} p_i^r(s_i - E_a) = n\sigma_n.$$

Moreover, since $\sum_{i=1}^n p_i^r(s) = 1$ and $p_i^r(s) > 0$, then

$$\min_i s_i - E_a \leq \sum_{i=1}^{n} p_i^r(s_i - E_a) \leq \max_i s_i - E_a.$$

The previous expression implies that $n\sigma_n$ is bounded; hence,

$$\lim_{n\to\infty} \sigma_n = 0.$$

For this reason p^r satisfies Theorem 2.

Now, let us assume by contradiction that there is a distribution $\tilde{p} \neq p^r$ that minimizes the number of attacks, given s and n. Since $\tilde{p}$ is different than p^r, then the bidders will use different strategies. In particular, the individuals with high expected payoff, $\tilde{p}_i^r(s)(s_i - E_a) > \sigma_n$, will sponsor more attacks. In a similar way, agents with $\tilde{p}_j(s)(s_j - E_a) < \sigma_n$ will reduce their attacks.

Since $\tilde{p}$ minimizes the number of attacks, then the total increment in the attacks (with respect to p^r) is lower than the total reduction. This implies that selecting a single contractor, rather than n, should reduce the number of attacks. However, this contradicts Theorem 1, because selecting multiple bidders indeed reduces the number of attacks. Therefore, we conclude that p^r is the best selection policy. □

Proof of Proposition 3. From (16) we get the following FOC for the optimality of the attack strategy a given some bid s and audit with probability β.

$$\frac{\partial \tilde{w}_i(s, a)}{\partial a_i} = p_i^r(s)\mathrm{E}[\pi_i] - \dot{b}\left(\sum_{j\in\mathcal{C}_r} a_j\right) - a_i\ddot{b}\left(\sum_{j\in\mathcal{C}_r} a_j\right) \leq 0,$$

where

$$\mathrm{E}[\pi_i] = r_i E_a \beta + (s_i - E_a)(1 - \beta).$$

From the previous equation it follows that $a_i = 0$ for all $i \in \mathcal{C}_r$ if

$$\beta \geq \frac{1}{p_i^r(s)} \frac{(s_i - E_a)p_i^r(s) - \dot{b}(0)}{s_i - (1 + r_i)E_a}.$$

Observe that the attacks are feasible if the expected profit exceeds the cost of an attack; hence, $(s_i - E_a)p_i^r(s) - \dot{b}(0) > 0$. Moreover, the asymmetric information guarantees that the payments without audits (s_i) exceed the fair compensation with them ($(1 + r_i)E_a$), that is, $s_i - (1 + r_i)E_a > 0$. Therefore, if $p_i^r(s) = 1/n$, we can guarantee zero attacks if

$$\beta \leq \frac{s_i - E_a - n\dot{b}(0)}{s_i - (1 + r_i)E_a} \quad (22)$$

for all $i \in \mathcal{C}_r$. Observe that (22) is linear decreasing with respect to n. □

Supplementary material

Supplementary material associated with this article can be found, in the online version, at 10.1016/j.ijcip.2019.05.006.

REFERENCES

[1] R. Zimmerman, C. E. Restrepo, N. Dooskin, J. Fraissinet, R. Hartwell, J. Miller, and W. Remington, "Diagnostic tools to estimate consequences of terrorism attacks against critical infrastructure," in *Proceedings of the U.S. Department of Homeland Security Conference, Working Together: Research and Development Partnerships in Homeland Security, Boston, MA*2005.

[2] Semana "Negocio redondo" http://www.semana.com/nacion/articulo/negocio-redondo/94315-3 Semana 2008, accessed February 1, 2016.

[3] Caracol radio "Capturan a funcionarios de una empresa que atentaba contra las torres eléctricas de ISA" http://caracol.com.co/radio/2009/06/15/judicial/1245050340_829038.htmlCaracol radio 2009, accessed February 1, 2016.

[4] B. Krebs, "Who is Anna-Senpai, the Mirai Worm Author?" Krebs on Security, 2017, accessed May 19, 2017. [Online]. Available: https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/
[5] Stratfor "Colombia: Rebel Attacks Shaping Economy, Elections." 2002, accessed April 20, 2018. [Online]. Available: https://www.stratfor.com/analysis/colombia-rebel-attacks-shaping-economy-elections
[6] "Massive blackout hits colombia after rebel attacks," CNN, March 2000, accessed September 30, 2018. [Online]. Available: http://www.latinamericanstudies.org/farc/blackout.htm
[7] B. Barton, *Energy security: managing risk in a dynamic legal and regulatory environment* Oxford University Press on Demand, 2004.
[8] Anselma, Adriaan "Electricity returns to southwestern Colombian town 16 days after FARC attack." 2012. [Online]. Available: http://colombiareports.com/electricity-returns-to-southwestern-colombian-town-16-days-after-farc-attack/
[9] N. Okonjo-Iweala, *Fighting Corruption Is Dangerous: The Story Behind the Headlines* MIT Press, 2018.
[10] R. B. Myerson, "Optimal auction design," *Mathematics of operations research* vol. 6, no. 1, pp. 58–73, 1981.
[11] N. Nisan, T. Roughgarden, É Tardos, and V. V. Vazirani, *Algorithmic Game Theory* 32 Avenue of the Americas, New York, NY 10013-2473, USA: Cambridge University Press, 2007.
[12] Congreso de Colombia "Ley 80 de 1993," 1993, accessed February 1, 2016. [Online]. Available: http://www2.igac.gov.co/igac_web/UserFiles/File/web%202008%20/ley%2080-93.pdf
[13] Congreso de Colombia, "Decreto 1510 de 2013," 2013, accessed February 1, 2016. [Online]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53776#163
[14] C. Barreto and A. A. Cárdenas, "Perverse incentives in security contracts: A case study in the colombian power grid," in *the Annual Workshop on the Economics of Information Security WEIS* 2016.
[15] G. Hardin, "The Tragedy of the Commons" *Science* vol. 162, no. 3859, pp. 1243–1248, Dec. 1968.
[16] C. H. Papadimitriou, "Algorithms, games, and the internet," in *In STOC* ACM Press, 2001, pp. 749–753.
[17] A. Shleifer, "A theory of yardstick competition," *The RAND Journal of Economics* pp. 319–327, 1985.
[18] P. Klemperer, "Why every economist should learn some auction theory," in *Advances in Economics and Econometrics: Invited Lectures to 8th World Congress of the Econometric Society* M. Dewatripont, L. Hansen, and S. Turnovsky, Eds. Cambridge University Press, 2003.
[19] El Tiempo "ELN retiene obreros de torres" El Tiempo 2000, accessed September 22, 2016. [Online]. Available: http://www.eltiempo.com/archivo/documento/MAM-1305561
[20] N. Falliere, L. O. Murchu, and E. Chien, *W32.Stuxnet Dossier* version 1.0 ed., Symantec, September 2010.
[21] K. Zetter, "Inside the cunning, unprecedented hack of ukraine's power grid," http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ WIRED magazine, mar 2016, accessed October 16, 2017.
[22] J. Finkle, "Hackers halt plant operations in watershed cyber attack," Reuters, 2017, accessed April 16, 2018. [Online]. Available: https://www.reuters.com/article/us-cyber-infrastructure-attack/hackers-halt-plant-operations-in-watershed-cyber-attack-idUSKBN1E8271
[23] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications* vol. 1, no. 1, pp. 13–27, 2016.
[24] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys & Tutorials* vol. 20, no. 4, pp. 3453–3495, 2018.
[25] S. Soltan, P. Mittal, and H. V. Poor, "Blackiot: Iot botnet of high wattage devices can disrupt the power grid," in *27th {USENIX} Security Symposium {USENIX} Security 18* 2018, pp. 15–32.
[26] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security TISSEC* vol. 14, no. 1, p. 13, 2011.
[27] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid* vol. 2, no. 4, pp. 659–666, 2011.
[28] L. Jia, R. J. Thomas, and L. Tong, "Malicious data attack on real-time electricity market," in *2011 IEEE International Conference on Acoustics, Speech and Signal Processing ICASSP* IEEE, 2011, pp. 5952–5955.
[29] C. Barreto and A. Cardenas, "Impact of the market infrastructure on the security of smart grids," *IEEE Transactions on Industrial Informatics* pp. 1–1, 2018.
[30] C. Barreto and A. A. Cárdenas, "Optimal risk management in critical infrastructures against cyber-adversaries," in *2017 IEEE Conference on Control Technology and Applications CCTA* Aug 2017, pp. 2027–2032.
[31] C. Barreto, A. A. Cardenas, and A. Bensoussan, "Optimal security investments in a prevention and detection game," in *Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp* ACM, Apr 2017, pp. 24–34.
[32] Z. Anwar, M. Montanari, A. Gutierrez, and R. H. Campbell, "Budget constrained optimal security hardening of control networks for critical cyber-infrastructures," *International Journal of Critical Infrastructure Protection* vol. 2, no. 1–2, pp. 13–25, 2009.
[33] J. Salmeron K. Wood and R. Baldick "Analysis of electric grid security under terrorist threat," *IEEE Transactions on Power Systems*vol. 19, no. 2, pp. 905–912, May 2004.
[34] E. Jenelius, J. Westin, and Å J. Holmgren, "Critical infrastructure protection under imperfect attacker perception," *International Journal of Critical Infrastructure Protection* vol. 3, no. 1, pp. 16–26, 2010.