Multifirm Models of Cybersecurity Investment Competition vs. Cooperation and Network Vulnerability

Anna Nagurney
Department of Operations and Information Management
Isenberg School of Management
University of Massachusetts Amherst
Shivani Shukla
Department of Business Analytics
School of Management
University of San Francisco

INFORMS Annual Meeting 2019
Seattle, WA

Cybersecurity and Homeland Security Policy

Outline

This presentation is based on the paper,
Nagurney, A., and Shukla, S. (2017). Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. European Journal of Operational Research, 260(2), 588-600,
where many references and additional theoretical and numerical results can be found.

Introduction

- An increasingly connected world may amplify the effects of a disruption.
- Estimated annual cost to the global economy from cybercrime is more than $400 billion, conservatively, $375 billion in losses, more than the national income of most countries (Center for Strategic and International Studies (2014)).

Introduction

- Growing interest in the development of **rigorous scientific tools**.
- As reported in Glazer (2015), JPMorgan was expected to double its cybersecurity spending in 2015 to $500 million from $250 million in 2014.
- According to Purnell (2015), the research firm Gartner reported in January 2015 that the global information security spending would increase by 7.6% in 2015 to $790 billion.
- It is clear that making the best **cybersecurity investments is a very timely problem and issue**.

Approach

- Three distinct models for cybersecurity investment in competitive and cooperative situations developed to safeguard against potential and ongoing threats.

Approach

- Three distinct models for cybersecurity investment in competitive and cooperative situations developed to safeguard against potential and ongoing threats.

Approach

- Three distinct models for cybersecurity investment in competitive and cooperative situations developed to safeguard against potential and ongoing threats.
- The first one captures non-cooperative behavior through **Nash Equilibrium (NE)**.

Approach

- Three distinct models for cybersecurity investment in competitive and cooperative situations developed to safeguard against potential and ongoing threats.
- The first one captures non-cooperative behavior through **Nash Equilibrium (NE)**.
- The second handles cooperation through the **Nash Bargaining (NB)** theory.

Approach

- Three distinct models for cybersecurity investment in competitive and cooperative situations developed to safeguard against potential and ongoing threats.
- The first one captures non-cooperative behavior through **Nash Equilibrium (NE)**.
- The second handles cooperation through the **Nash Bargaining (NB)** theory.
- Finally, the third model takes a systems perspective and captures cooperation through **System-Optimization (S-O)**.

Important References:

Nagurney, A. (2015). A multiproduct network economic model of cybercrime in financial services. *Service Science*, 7(1), 70-81.

Nagurney, A., Nagurney, L.S., Shukla, S. (2015). A supply chain game theory framework for cybersecurity investments under network vulnerability. In *Computation, Cryptography, and Network Security*, Daras, Nicholas J., Rassias, Michael Th. (Eds.), Springer, 381-398.

Nagurney A., Daniele P., Shukla S. (2016). A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints, *to appear in Annals of Operations Research*.

The Multifirm Cybersecurity Investment Models: Common Features

Network Security, s_i:

$$0 \leq s_i \leq u_{s_i}; \quad i = 1, ..., m.$$

$u_{s_i} < 1$: Upper bound on security level of firm i.

Average Network Security of the Chain, $\bar{s}$:

$$\bar{s} = \frac{1}{m} \sum_{i=1}^{m} s_i.$$

Probability of a Successful Cyberattack on i, p_i:

$$p_i = (1 - s_i)(1 - \bar{s}), \quad i = 1, ..., m.$$

Vulnerability, v_i:

$v_i = (1 - s_i), \quad i = 1, ..., m.$ Vulnerability of network, $\bar{v} = (1 - \bar{s})$.

The Multifirm Cybersecurity Investment Models: Common Features

Investment Cost Function to Acquire Security s_i, $h_i(s_i)$:

$$h_i(s_i) = \alpha_i(\frac{1}{\sqrt{(1-s_i)}} - 1), \quad \alpha_i > 0, \qquad i = 1, ..., m.$$

α_i quantifies size and needs of retailer i; $h_i(0) = 0 =$ insecure retailer, and $h_i(1) = \infty =$ complete security at infinite cost.

Incurred financial damage if attack successful: D_i.
Expected Financial Damage after Cyberattack for Firm i; $i = 1, ..., m$:

$$D_i p_i, \qquad D_i \geq 0.$$

The Multifirm Cybersecurity Investment Models: Common Features

Each firm $i; i = 1, ..., m$ has a utility associated with its wealth W_i, denoted by $f_i(W_i)$, which is increasing, and is continuous and concave. The form of the $f_i(W_i)$ that we use in this paper is $\sqrt{W_i}$ (see Shetty et al. (2009)). Such a function is increasing, continuous, and concave, reflecting that a firm's wealth has a positive but decreasing marginal benefit.

Expected Utility/Profit for Firm $i, i = 1, ..., m$:

$$E(U_i) = (1 - p_i)f_i(W_i) + p_i(f_i(W_i) - D_i) - h_i(s_i).$$

Each $E(U_i(s))$ is strictly concave with respect to s_i and each $h_i(s_i)$ is strictly convex.

The Nash Equilibrium Model of Cybersecurity Investments

We seek to determine a security level pattern $s \in K^1$, where $K^1 = \prod_{i=1}^{m} K_i^1$ and $K_i^1 \equiv \{s_i | 0 \leq s_i \leq u_{s_i}\}$, such that the firms will be in a state of equilibrium with respect to their cybersecurity levels.

Definition 1: Nash Equilibrium in Cybersecurity Levels

A security level pattern $s^* \in K^1$ is said to constitute a cybersecurity level Nash equilibrium if for each firm i; $i = 1, \ldots, m$:

$$E(U_i(s_i^*, \hat{s}_i^*)) \geq E(U_i(s_i, \hat{s}_i^*)), \quad \forall s_i \in K_i^1,$$

where

$$\hat{s_i^*} \equiv (s_1^*, \ldots, s_{i-1}^*, s_{i+1}^*, \ldots, s_m^*).$$

Variational Inequality Formulation

Theorem 1: Variational Inequality Formulation of Nash Equilibrium in Cybersecurity Levels

$s^* \in K^1$ is a Nash equilibrium in cybersecurity levels according to Definition 1 if and only if it satisfies the variational inequality

$$-\sum_{i=1}^{m} \frac{\partial E(U_i(s^*))}{\partial s_i} \times (s_i - s_i^*) \geq 0, \quad \forall s \in K^1,$$

or, equivalently,

$$\sum_{i=1}^{m} \left[\frac{\partial h_i(s_i^*)}{\partial s_i} + [f_i(W_i) - f_i(W_i - D_i)] \left[\frac{1}{m} \sum_{j=1}^{m} s_j^* - 1 - \frac{1}{m} + \frac{s_i^*}{m} \right] \right] \times (s_i - s_i^*) \geq 0,$$

$$\forall s \in K^1.$$

The Nash Bargaining Model of Cybersecurity Investments

The bargaining model proposed by Nash (1950b, 1953) is based on axioms and focused on two players, that is, decision-makers. The framework easily generalizes to m decision-makers, as noted in Leshem and Zehavi (2008). $E(U_j^{NE})$, evaluated at NE, is the disagreement point of firm j, according to the bargaining framework.

The optimization problem to be solved is:

$$\text{Maximize} \prod_{j=1}^{m} (E(U_j(s)) - E(U_j^{NE}))$$

subject to:

$$E(U_j(s)) \geq E(U_j^{NE}), \quad j = 1, \ldots, m,$$

$$s \in K^1.$$

We define the feasible set K^2 consisting of all constraints, which we know is convex.

The System-Optimization Model of Cybersecurity Investments

The system-optimization cybersecurity investment problem is to:

$$\text{Maximize} \sum_{j=1}^{m} E(U_j(s))$$

subject to:

$$s \in K^1.$$

We know that feasible set is convex and compact and that the objective function is continuous. Hence, the solution to the above system-optimization problem is guaranteed to exist.

Numerical Case Studies

- Solutions of the Nash Equilibrium model were computed by applying the Euler method.
- The convergence tolerance was set to 10^{-5}, so that the algorithm was deemed to have converged when the absolute value of the difference between each successively computed security level was less than or equal to 10^{-5}.
- The sequence $\{a_\tau\}$ was set to: $.1\{1, \frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}, ...\}$.
- The upper bounds on the security levels $u_{s_i} = 0.99, \forall i$.
- The solutions to the Nash Bargaining and System-Optimization models were computed by applying the Interior Point Method in the SAS NLP Solver.
- The algorithm was called upon while using SAS Studio.
- Optimality errors of S-O is 5×10^{-7}.

Case I: Retailers

- Consider two retailers. Firm 1 represents **Target Corporation**.
- Credit card information of 40 million users was used by hackers to generate an estimated $53.7 million in the black market as per Newsweek (2014).
- Suffered $148 million in damages.
- Firm 2 represents **The Home Depot**. It incurred $62 million in legal fees and staff overtime to deal with their cyber attack in 2014. Additionally, it paid $90 million to banks for re-issuing debit and credit cards to users who were compromised (Newsweek (2014)).
- We use the annual revenue data for the firms to estimate their wealth.

Case I: Retailers

Hence, in US$ in millions, $W_1 = 72600$; $W_2 = 78800$. The potential damages these firms stand to sustain in the case of similar cyberattacks as above in the future amount to (in US$ in millions): $D_1 = 148.0$; $D_2 = 152$. Wwealth functions are of the following form:

$$f_1(W_1) = \sqrt{W_1}; \quad f_2(W_2) = \sqrt{W_2}.$$

The cybersecurity investment cost functions are:

$$h_1(s_1) = 0.25(\frac{1}{\sqrt{1-s_1}} - 1); \quad h_2(s_2) = 0.30(\frac{1}{\sqrt{1-s_2}} - 1).$$

The parameters $\alpha_1 = .25$ and $\alpha_2 = .30$ are the number of employees of the respective firms in millions.

Case I: Retailers

Results:

Solution	NE	NB	S-O
s_1^*	0.384	0.443	0.460
s_2^*	0.317	0.409	0.388
v_1	0.616	0.557	0.540
v_2	0.683	0.591	0.612
$\bar{s}^*$	0.350	0.426	0.424
$\bar{v}$	0.650	0.574	0.576
$E(U_1)$	269.265	269.271	269.268
$E(U_2)$	280.530	280.531	280.534

Table: Results for NE, NB, and S-O for Target and Home Depot

Case I: Retailers

Target Corporation is part of the Retail Cyber Intelligence Sharing Center through which the firm shares cyber threat information with other retailers that are part of the Retail Industry Leaders Association and also with public stakeholders such as the U.S. Department of Homeland Security, and the F.B.I (RILA (2014)). Even Home Depot has expressed openness towards the sharing threat information.

Case I: Sensitivity Analysis

To examine the magnitude of changes in network vulnerability and expected utilities, for varying damages, same wealth, and $\alpha_1 = 100, \alpha_2 = 120$, we present:

Parameters		NE		NB		S-O	
D_1	D_2	$E(U_1)$	$E(U_2)$	$E(U_1)$	$E(U_2)$	$E(U_1)$	$E(U_2)$
24800	25200	222.472	235.991	223.541	237.087	223.410	237.220
34800	35200	210.460	223.098	211.619	224.278	211.517	224.381
44800	45200	200.039	212.090	201.276	213.340	201.212	213.405

Table: Expected Utilities for NE, NB, and S-O for Target and Home Depot

Parameters		NE			NB			S-O		
D_1	D_2	s_1^*	s_2^*	$\bar{v}$	s_1^*	s_2^*	$\bar{v}$	s_1^*	s_2^*	$\bar{v}$
24800	25200	.169	.066	.88285	.262	.164	.78711	.265	.161	.78719
34800	35200	.289	.197	.75705	.369	.281	.67496	.371	.279	.67502
44800	45200	.374	.288	.66915	.444	.363	.59661	.445	.362	.59665

Table: Network Vulnerability $\bar{v}$ for NE, NB, and S-O for Target and Home Depot

Case I: Sensitivity Analysis

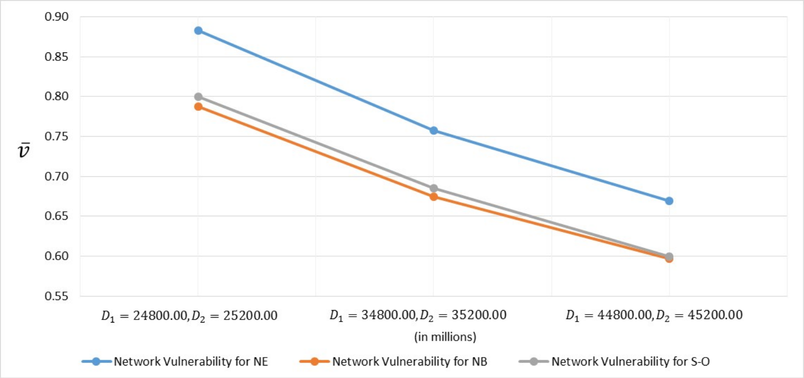

Figure: Comparison of Network Vulnerability $\bar{v}$ for NE, NB, and S-O with Varying D_i Parameters with $\alpha_1 = 100$ and $\alpha_2 = 200$

Case II: Financial Service Firms

- In Case II, we consider three banking and financial service firms.
- Firm 1 represents **JPMorgan Chase (JPMC)**.
- More than 76 million households and seven million small businesses were compromised - hackers manipulated apps and programs for alternate entry (The New York Times (2014)).
- Firm 2 represents **Citibank**, part of Citigroup.
- Breach in 2011 in which 34,000 of the company's customers were affected - Financial losses were compensated and 217,657 credit cards were replaced (Neowin (2011)).
- Firm 3 is represented by **HSBC Holdings Plc's Turkish Unit**.
- The unit was attacked right after JPMC in 2014 and 2.7 million customers' bank data was lost (Bloomberg (2014)).

Case II: Financial Service Firms

In US$ in millions, $W_1 = 51500$; $W_2 = 33300$; $W_3 = 31100$. The potential damages these firms could stand to sustain in the future, in the case of similar cyberattacks to those described above, amount to (in US$ in millions): $D_1 = 250.00$; $D_2 = 172.80$; $D_3 = 580.50$.
The wealth functions are:

$$f_1(W_1) = \sqrt{W_1}; \quad f_2(W_2) = \sqrt{W_2}; \quad f_2(W_3) = \sqrt{W_3}.$$

The cybersecurity investment cost functions take the form:

$$h_1(s_1) = 0.27(\frac{1}{\sqrt{1-s_1}} - 1); \quad h_2(s_2) = 0.24(\frac{1}{\sqrt{1-s_2}} - 1);$$

$$h_1(s_3) = 0.27(\frac{1}{\sqrt{1-s_3}} - 1).$$

Case II: Financial Service Firms

Results:

Solution	NE	NB	S-O
s_1^*	0.467	0.542	0.581
s_2^*	0.454	0.535	0.598
s_3^*	0.719	0.762	0.718
v_1	0.533	0.458	0.419
v_2	0.547	0.465	0.402
v_3	0.281	0.238	0.282
$\bar{s}^*$	0.546	0.613	0.632
$\bar{v}$	0.454	0.387	0.368
$E(U_1)$	226.703	226.709	226.704
$E(U_2)$	182.281	182.286	182.274
$E(U_3)$	175.902	175.916	175.942

Table: Results of NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit

Case II: Financial Service Firms

Quantum Dawn 2 and 3 are cybersecurity incident response drills conducted for enhancing resolution and coordination processes in the financial services sector. These exercises are meant to avoid ripple effects of a cyberattack on one firm to others. To counteract such coordinated attacks, the financial service firms and banks realize the importance of sharing information and protect through a coordinated response (SIFMA (2015)). Our results on the Nash bargaining corroborate this understanding, support negotiations, and numerically reveal the increase in security levels and the concomitant decrease in network vulnerability.

Case II: Sensitivity Analysis

Wealth parameters are the same but damage parameters increased to $D_1 = 25000.00$, $D_2 = 17200.80$, $D_3 = 28000.50$, and the alpha parameters varying in an elevated range.

Parameters			NE			NB			S-O		
α_1	α_2	α_3	$E(U_1)$	$E(U_2)$	$E(U_3)$	$E(U_1)$	$E(U_2)$	$E(U_3)$	$E(U_1)$	$E(U_2)$	$E(U_3)$
75	65	75	183.14	144.52	105.42	184.64	145.83	107.88	184.04	144.02	111.11
100	90	100	177.13	139.29	92.33	179.05	140.96	95.45	178.28	138.70	99.500
150	125	150	170.46	133.22	72.74	173.07	135.46	76.99	172.03	132.29	82.64

Table: Expected Utilities for NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit

Parameters			NE				NB				S-O			
α_1	α_2	α_3	s_1^*	s_2^*	s_3^*	$\bar{v}$	s_1^*	s_2^*	s_3^*	$\bar{v}$	s_1^*	s_2^*	s_3^*	$\bar{v}$
75	65	75	.258	.258	.484	.667	.366	.366	.564	.568	.392	.423	.513	.557
100	90	100	.169	.151	.423	.752	.291	.275	.512	.641	.319	.339	.456	.629
150	125	150	.018	.040	.318	.875	.161	.180	.423	.745	.195	.257	.356	.731

Table: Network Vulnerability $\bar{v}$ for NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit

Case II: Sensitivity Analysis

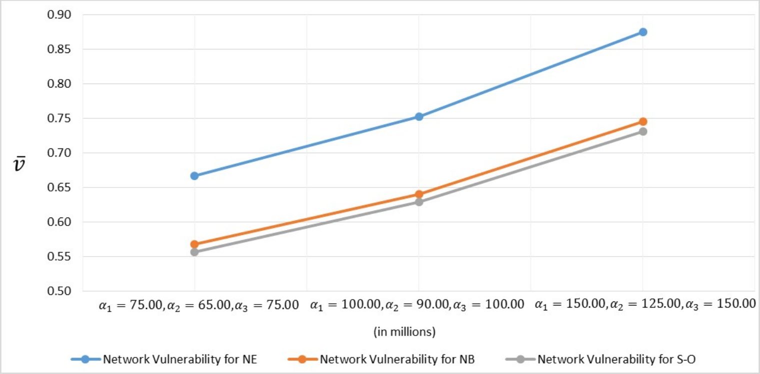

Figure: Comparison of Network Vulnerability $\bar{v}$ for NE, NB, and S-O with Varying α_i Parameters with $D_1 = 25000.00$, $D_2 = 17200.80$ and $D_3 = 28000.50$

Case III: Energy Firms

- Cyber espionage assaults targeting the energy sector have seen a sharp rise since 2007, making it the top target as of 2014.
- In Case III, we consider three internationally renowned oil and gas companies.
- Firm 1 represents **Royal Dutch Shell Plc**. **British Petroleum (BP)** is Firm 2, and Firm 3 is **Exxon Mobil**.
- Since the actual damage was confidential and not reported, we have estimated it by multiplying the throughput of each of these firms (barrels produced per day for six months) with the oil price of $53.5.

Case III: Energy Firms

In US$ in millions, we let $W_1 = 293290$; $W_2 = 234250$; $W_3 = 437640$. The potential damages these firms could stand to sustain amount to (in US$ in millions): $D_1 = 38080.40$; $D_2 = 40033.10$; $D_3 = 51750.30$.
The wealth functions are:

$$f_1(W_1) = \sqrt{W_1}; \quad f_2(W_2) = \sqrt{W_2}; \quad f_2(W_3) = \sqrt{W_3}.$$

The cybersecurity investment cost functions take the form:

$$h_1(s_1) = 0.094(\frac{1}{\sqrt{1-s_1}} - 1); \quad h_2(s_2) = 0.075(\frac{1}{\sqrt{1-s_2}} - 1);$$

$$h_1(s_3) = 0.085(\frac{1}{\sqrt{1-s_3}} - 1).$$

Case III: Energy Firms

Results:

Solution	NE	NB	S-O
s_1^*	0.936	0.945	0.946
s_2^*	0.949	0.957	0.956
s_3^*	0.943	0.951	0.951
v_1	0.064	0.055	0.054
v_2	0.051	0.043	0.044
v_3	0.057	0.049	0.049
$\bar{s}^*$	0.942	0.951	0.951
$\bar{v}$	0.058	0.049	0.049
$E(U_1)$	541.151	541.157	541.156
$E(U_2)$	483.609	483.615	483.617
$E(U_3)$	661.142	661.150	661.149

Table: Results for NE, NB, and S-O for Shell, BP, and Exxon Mobil

Case III: Energy Firms

LOGIIC, Linking the Oil and Gas Industry to Improve Cybersecurity, was established for collaboration between companies in this sector and the US Department of Homeland Security. BP, Chevron, Shell, Total and others possessing global energy infrastructure are members of the program (Automation Federation (2013)). We note that the optimality error for the NB solution for this case was 7.85×10^{-9}.

Case III: Sensitivity Analysis

Damage parameters are increased three-fold to $D_1 = 114241.20, D_2 = 120099.30, D_3 = 155250.90$ and the alpha parameters are increased to $\alpha_1 = 225, \alpha_2 = 75, \alpha_3 = 195$. Such increases represent more damaging attacks on firms bigger in size or needs with dwindling wealth.

Case III: Sensitivity Analysis

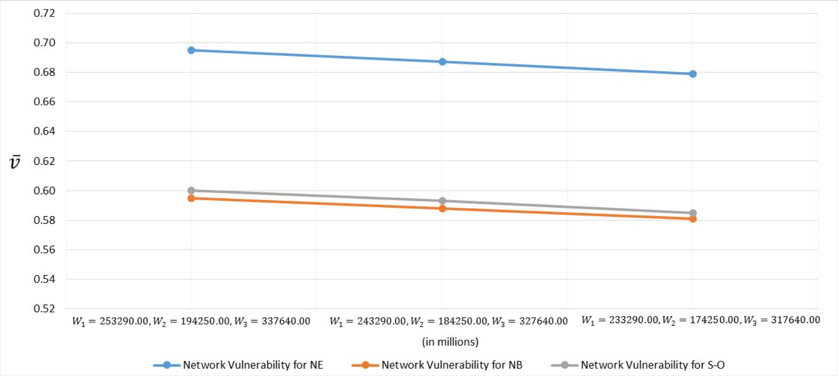

Figure: Comparison of Network Vulnerability $\bar{v}$ for NE, NB, and S-O and Varying W_i Parameters with $D_1 = 114241.20, D_2 = 120099.30, D_3 = 155250.90$, and $\alpha_1 = 225, \alpha_2 = 75, \alpha_3 = 195$

Summary and Conclusions

- In Case I, **as damages increase, network vulnerability decreases**. NB solution concept yields the lowest network vulnerability.

Summary and Conclusions

- In Case I, **as damages increase, network vulnerability decreases**. NB solution concept yields the lowest network vulnerability.
- In Case II, **as the number of employees increase**, which, consequently, increases the investment cost functions, and the damages remain the same, **firms invest less in security**.

Summary and Conclusions

- In Case I, **as damages increase, network vulnerability decreases**. NB solution concept yields the lowest network vulnerability.
- In Case II, **as the number of employees increase**, which, consequently, increases the investment cost functions, and the damages remain the same, **firms invest less in security**.
- In Case III, **as the wealth decreases**, firms become more vulnerable to damages and, thus, invest more into security which leads to **higher security levels**. NB solution concept yields the lowest network vulnerability.
- Network vulnerability of NB not the lowest but **expected utility of Firm 2 falls below NE**.

Summary and Conclusions

- In Case I, **as damages increase, network vulnerability decreases**. NB solution concept yields the lowest network vulnerability.
- In Case II, **as the number of employees increase**, which, consequently, increases the investment cost functions, and the damages remain the same, **firms invest less in security**.
- In Case III, **as the wealth decreases**, firms become more vulnerable to damages and, thus, invest more into security which leads to **higher security levels**. NB solution concept yields the lowest network vulnerability.
- Network vulnerability of NB not the lowest but **expected utility of Firm 2 falls below NE**.
- **Nash Bargaining model is the most practical and beneficial** for firms, the network, and consumers alike in terms of security levels.

Acknowledgements

- This research of the first author was supported by the National Science Foundation (NSF) grant CISE #1111276, for the NeTS: Large: Collaborative Research: Network Innovation Through Choice project awarded to the University of Massachusetts Amherst. This support is gratefully acknowledged.

Thank You!

For more information, please visit:
http://supernet.isenberg.umass.edu/default.htm.