Multifirm Models of Cybersecurity Investments Competition Vs. Cooperation

Anna Nagurney

Isenberg School of Management
University of Massachusetts Amherst

Shivani Shukla

School of Management
University of San Francisco

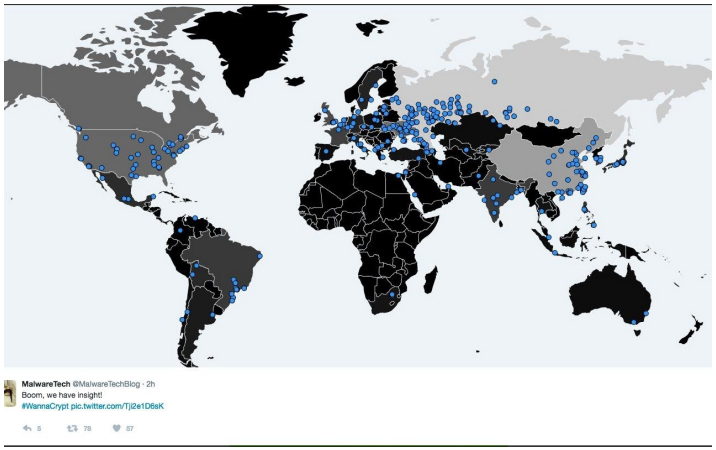
INFORMS Annual Meeting, Houston, Texas

October 22-25, 2017

Introduction

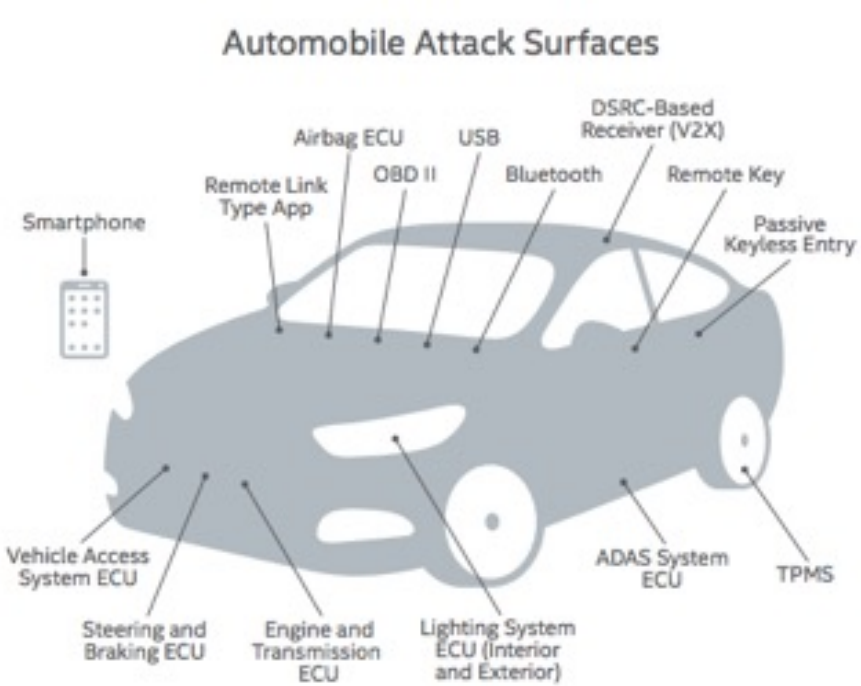
The barrage of cyberattacks in 2017:

- Equifax: May have affected 143 million customers. Names, SSNs, birthdates, drivers' license information, and 209K credit card numbers Lasted between mid-May to July (Bloomberg (2017)).
- Ransomware "WannaCry": Crippled National Health Services Hospitals in the UK. Hobbling emergency rooms, delaying vital medical procedures, and creating chaos (Wired (2017)).



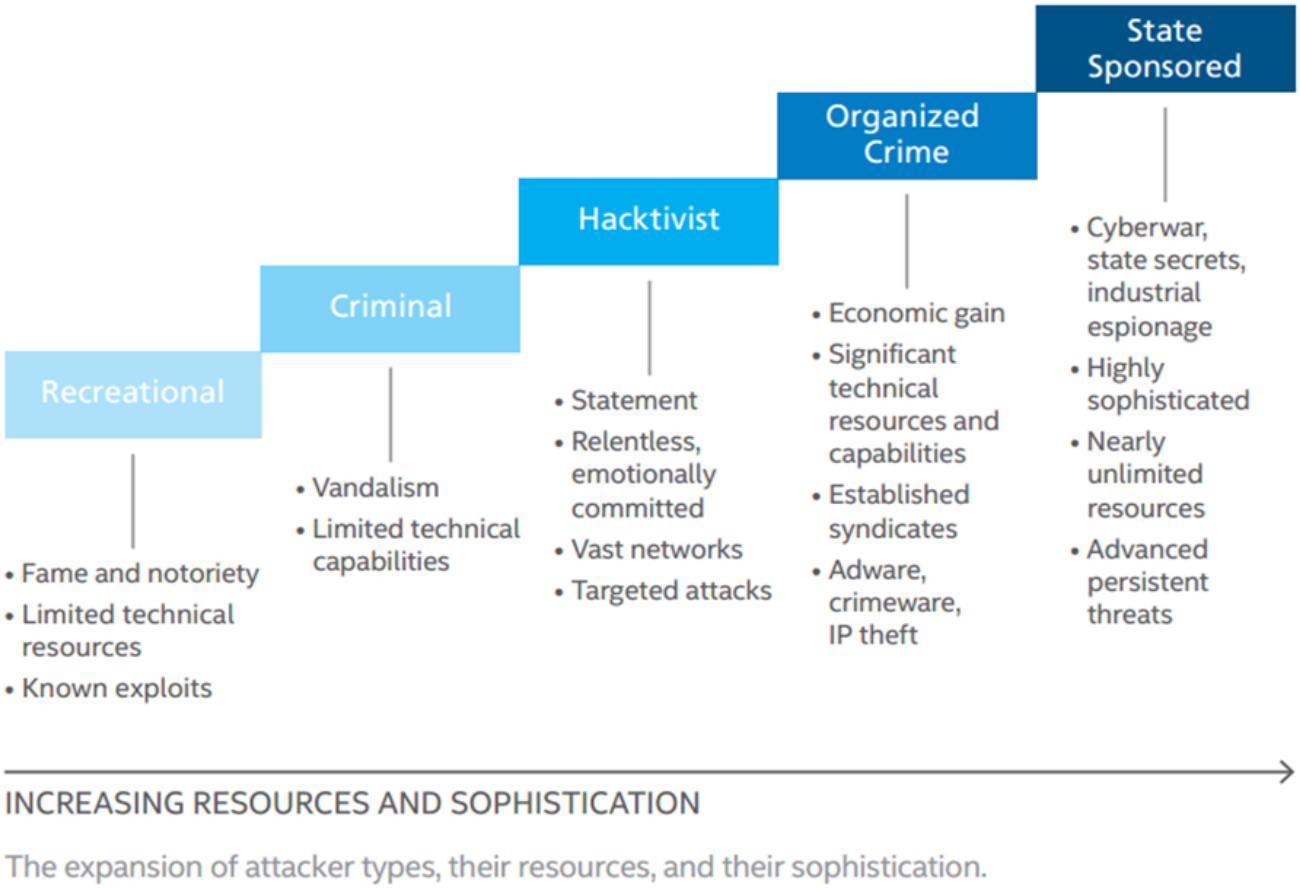
Introduction

- Discovery of a Publicly Accessible Database: 198 million US voters' information. Possibly every voter going back 10 years (Wired (2017)).
- Pentagon: High-Speed traders used to study how hackers could unleash chaos in the financial system (The Wall Street Journal (2017)).



Fifteen of the most hackable and exposed attack surfaces, including several electronic control units, on a next-generation car.

Changing Attacker Profiles



The expansion of attacker types, their resources, and their sophistication.

Source: McAfee Labs Threats Report (2015)

Cooperation against Large-Scale Attacks

- Bilateral cybersecurity cooperation among US and Japan, particularly for Botnets.
- Stress on upcoming 2020 Olympics.
- Military cooperation - Joint cyberdefense working group since 2013 (The Hill (2017)).
- Ransomware proliferation and effective tactics for business-law enforcement cooperation on cybersecurity (CSIS (2017)).
- Japan and Singapore: Information exchanges, collaborations to enhance cybersecurity awareness, joint regional capacity-building efforts, and sharing of best practices (The Japan Times (2017)).
- It will take a planet!

Literature Review

Theoretical Development of Nash Bargaining Theory

- Nash J.F. (1950b). The bargaining problem. *Econometrica*, 18, 155-162.
- Harsanyi, J. C. (1963). A simplified bargaining model for the n-person cooperative game. *International Economic Review*, 4(2), 194-220.
- Muthoo A. (1999). *Bargaining Theory with Applications*. Cambridge, England: Cambridge University Press.
- Harrington J.E., Hobbs B.F., Pang J.S., Liu A., & Roch G. (2005). Collusive game solutions via optimization. *Mathematical Programming*, 104(2-3): 407-435.
- Nagarajan M., & Sosic G. (2008). Game-theoretic analysis of cooperation among supply chain agents: Review and extensions. *European Journal of Operational Research*, 187(3), 719-745.
- Bakshi N, & Kleindorfer P. (2009). Co-opetition and investment for supply-chain resilience. *Production and Operations Management*, 18(6), 583-603.

This presentation is based on the following paper:

Nagurney, A., & Shukla, S. (2017). Multifirm Models of Cybersecurity Investment Competition vs. Cooperation and Network Vulnerability. *European Journal of Operational Research*, 260(2), 588-600.

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)**.

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, $h_i(s_i)$:

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

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; $i = 1, ..., m$:

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

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 is used 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 $h_i(s_i)$ 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,

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

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

Existence

We define the m-dimensional vectors $X \equiv s$ and $F(X)$ with the i-th component, F_i, of $F(X)$ given by

$$F_i(X) \equiv -\frac{\partial E(U_i(s))}{\partial s_i}$$

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

and with the feasible set $\mathcal{K} \equiv K^1$ and $N = m$. The variational inequality described earlier can, thus, be put into the standard form.

A solution to variational inequality for the Nash equilibrium cybersecurity investment model is guaranteed to exist since the function $F(X)$ is **continuous** and the **feasible set** $\mathcal{K} = K^1$ **is compact** (see Kinderlehrer and Stampacchia (1980) and Nagurney (1999))

Uniqueness of the Nash Equilibrium

Theorem 2: Uniqueness of the Nash Equilibrium

If $F(X)$ is strictly monotone, that is:

$$\langle (F(X^1) - F(X^2)), X^1 - X^2 \rangle > 0, \quad \forall X^1, X^2 \in \mathcal{K}, X^1 \neq X^2,$$

then X^*, the solution to variational inequality described earlier, is unique.

Condition for the Strict Diagonal Dominance of the Jacobian

We know that if the Jacobian of $F(X)$, which is denoted by J, is positive definite, then $F(X)$ is strictly monotone.
It then follows that

$$J = \begin{bmatrix} \frac{3\alpha_1}{4(1-s_1)^{2.5}} + \frac{2}{m}[f_1(W_1) - f_1(W_1 - D_1)] & \cdots & \frac{1}{m}[f_1(W_1) - f_1(W_1 - D_1)] \\ \vdots & & \vdots \\ \frac{1}{m}[f_m(W_m) - f_m(W_m - D_m)] & \cdots & \frac{3\alpha_m}{4(1-s_m)^{2.5}} + \frac{2}{m}[f_m(W_m) - f_m(W_m - D_m)] \end{bmatrix}$$

From the structure of $(J + J^T)/2$ it can be inferred that it is strictly diagonally dominant if, $\forall i$:

$$\frac{3\alpha_i}{4(1-s_i)^{2.5}} > \frac{m-5}{2m}[f_i(W_i) - f_i(W_i - D_i)] + \frac{1}{2m}\sum_{j=1;j\neq i}^{m}[f_j(W_j) - f_j(W_j - D_j)].$$

Interpretation of the Condition for $m = 2$, $m = 3$

The condition will be satisfied, for example, for $m = 3$, if $2[f_i(W_i) - f_i(W_i - D_i)] \geq \sum_{j=1}^{m}[f_j(W_j) - f_j(W_j - D_j)], j \neq i$.

For $m = 2$ if the following conditions are satisfied then strict diagonal dominance of $(J + J^T)/2$ also holds:

$$3(f_1(W_1) - f_1(W_1 - D_1)) \geq f_2(W_2) - f_2(W_2 - D_2) \geq \frac{f_1(W_1) - f_1(W_1 - D_1)}{3}.$$

Of course, **positive-definiteness of J can still hold even when the strict diagonal dominance condition does not**.

The Euler Method

In view of the simple structure of the underlying feasible set, the Euler method yields at each iteration closed form expressions for the security levels: i; $i = 1, \ldots, m$, given by:

$$s_i^{\tau+1} = \max\{0, \min\{u_{s_i},$$

$$s_i^{\tau} + a_{\tau}(-\frac{\partial h_i(s_i^{\tau})}{\partial s_i^{\tau}} - (f_i(W_i) - f_i(W_i - D_i)) \left[\frac{1}{m}\sum_{j=1}^{m} s_j^{\tau} - 1 - \frac{1}{m} + \frac{s_i^{\tau}}{m}\right]\}\}.$$

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:

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

subject to:

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

Feasible set is defined as K^2 consisting of all constraints, which is known to be convex.

Uniqueness of the Nash Bargaining Solution

Theorem 3: Uniqueness of the Nash Bargaining Solution

The solution to the above cooperative Nash bargaining model is unique if the objective function, Z^1, is strictly quasi-concave.

We can transform Z^1 through the following logarithmic transformation:

$$ln(Z^1) = ln(\prod_{j=1}^{m}(E(U_j(s)) - E(U_j^{NE}))) = \sum_{j=1}^{m} ln(E(U_j(s)) - E(U_j^{NE})).$$

The objective function Z^1 is strictly quasi-concave if $ln(Z^1)$ is strictly concave.

The System-Optimization Model of Cybersecurity Investments

The system-optimization cybersecurity investment problem is to:

$$\text{Maximize } Z^2 = \text{Maximize} \sum_{j=1}^{m} E(U_j(s))$$

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.

Uniqueness of the System-Optimized Solution

Theorem 4: Uniqueness of the System-Optimized Solution

The solution to the system-optimization problem above is unique if the objective function, Z^2, is strictly concave.

Z^2 is strictly concave if its Hessian matrix, H, is negative definite or $-H$ is positive definite (for all feasible s), where

$$H = \begin{bmatrix} \frac{\partial^2 Z^2}{\partial s_1^2} & \cdots & \frac{\partial^2 Z^2}{\partial s_1 \partial s_m} \\ \vdots & & \vdots \\ \frac{\partial^2 Z^2}{\partial s_m \partial s_1} & \cdots & \frac{\partial^2 Z^2}{\partial s_m^2} \end{bmatrix}$$

Condition for the Strict Diagonal Dominance of the Hessian

The matrix is symmetric. Moreover, we know that $-H$ is positive definite if it is strictly diagonally dominant, with the satisfaction of the condition below:

$$\frac{3\alpha_j}{4(1-s_j)^{2.5}} > \frac{m-3}{m}[f_j(W_j) - f_j(W_j - D_j)]$$

$$+\frac{1}{m}\sum_{k=1;k\neq j}^{m}[f_k(W_k) - f_k(W_k - D_k)], \quad j = 1, \ldots, m.$$

The above condition is satisfied **for** $m = 2$ when $[f_i(W_i) - f_i(W_i - D_i)] = [f_j(W_j) - f_j(W_j - D_j)], \forall j \neq i$. If this relationship is true, **strict diagonal dominance will always exist for two firms**.

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 are 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): $D_1 = 148.0$; $D_2 = 152$.
Wealth 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: 1: 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.

Checking Uniqueness

NE: $b_i = \frac{3\alpha_i}{4(1-s_i)^{2.5}}$, and $c_i = \frac{m-5}{2m}[f_i(W_i) - f_i(W_i - D_i)] + \frac{1}{2m}\sum_{j=1;j\neq i}^{m}[f_j(W_j) - f_j(W_j - D_j)]$ for $i = 1, 2$. Hence, b_1 at $s_1 = 0$, is equal to **.188, and** c_1**=-.138**. Similarly, b_2 at $s_2 = 0$, is equal to **.225 and** c_2**=-.134**. Clearly, $b_1 > c_1$ and $b_2 > c_2$.

NB: The **lowest eigenvalue** of minus the Hessian evaluated at the computed NB solution was: **321.315**.

S-O: d_i: $g_i = \frac{m-3}{m}[f_i(W_i) - f_i(W_i - D_i)] + \frac{1}{m}\sum_{j=1;j\neq i}^{m}[f_j(W_j) - f_j(W_j - D_j)]$, $i = 1, 2$. I know, from the above computation, that b_1**=.188, and** g_1**=-.002**. Also, I know that b_2**=.225, from the above, with** g_2**=.002**. Clearly, $b_1 > g_1$ and $b_2 > g_2$

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: 2: Expected Utilities for NE, NB, and S-O for Target and Home Depot with $\alpha_1 = 100$ and $\alpha_2 = 120$

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: 3: Network Vulnerability $\bar{v}$ for NE, NB, and S-O for Target and Home Depot with $\alpha_1 = 100$ and $\alpha_2 = 120$

Case I: Sensitivity Analysis

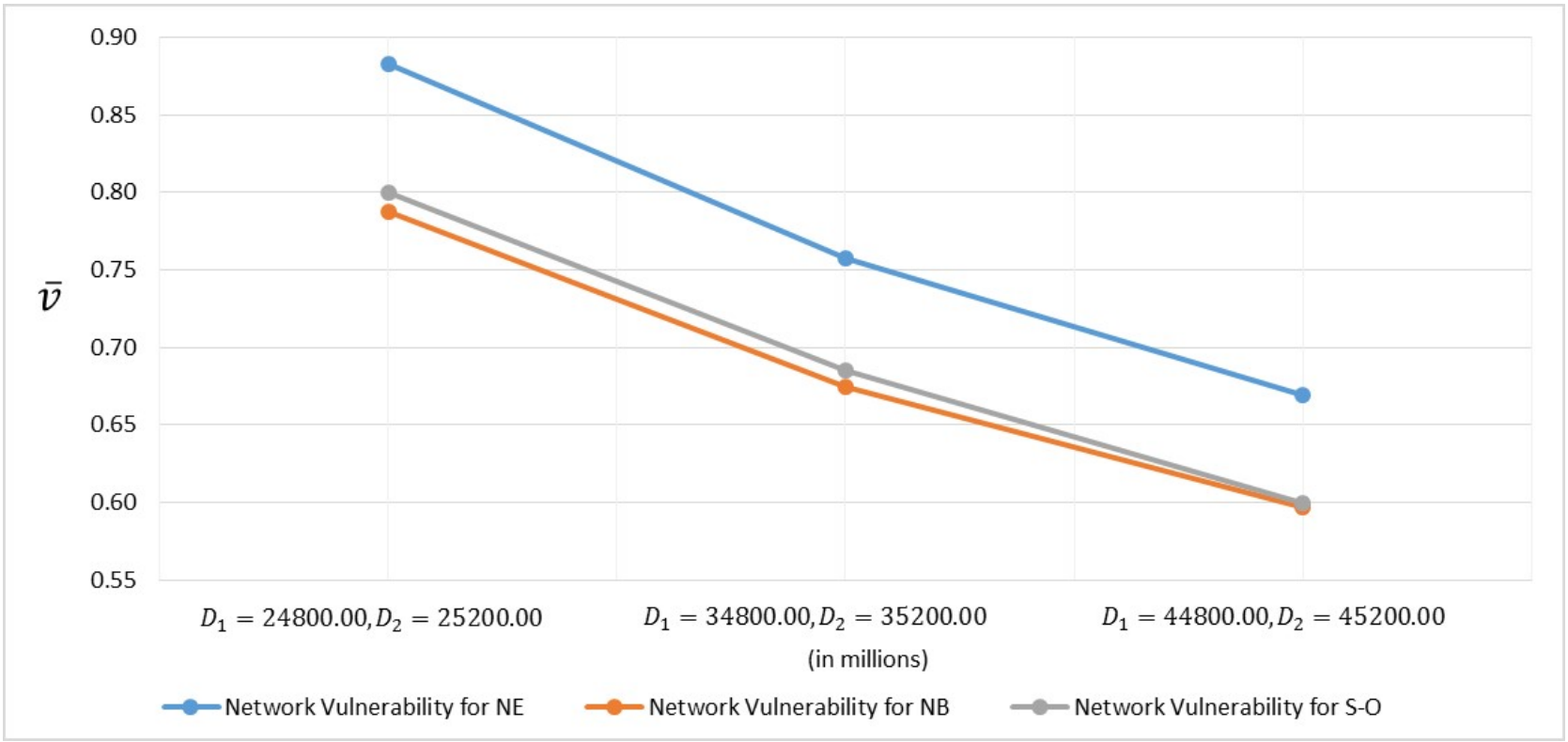


Figure: 1: Comparison of Network Vulnerability $\bar{v}$ for NE, NB, and S-O with Varying D_i Parameters with $\alpha_1 = 100$ and $\alpha_2 = 120$

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:

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

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

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: 4: 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 (SIFMA (2015)). My 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.

Checking Uniqueness

NE: I have that: b_1=**.202,** c_1=**.171,** b_2=**.180,** c_2=**.209, and** b_3=**.520, with** c_3=**-.380**. Clearly, for this example: $\mathbf{b_1} > \mathbf{c_1}$ and $\mathbf{b_3} > \mathbf{c_3}$. However, $\mathbf{b_2} < \mathbf{c_2}$. I evaluate the eigenvalues for $\frac{1}{2}(J + J^T)$ and find that the **smallest eigenvalue is positive and equal to .699**.

NB: The **lowest eigenvalue** of minus the Hessian evaluated at the computed NB solution was: **501.665**.

S-O: The **smallest eigenvalue** of this matrix is positive and equal to **.044**.

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: 5: Expected Utilities for NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit with $D_1 = 25000.00, D_2 = 17200.80$ and $D_3 = 28000.50$

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: 6: Network Vulnerability $\bar{v}$ for NE, NB, and S-O for JPMC, Citibank, and HSBC Turkish Unit with $D_1 = 25000.00, D_2 = 17200.80$ and $D_3 = 28000.50$

Case II: Sensitivity Analysis

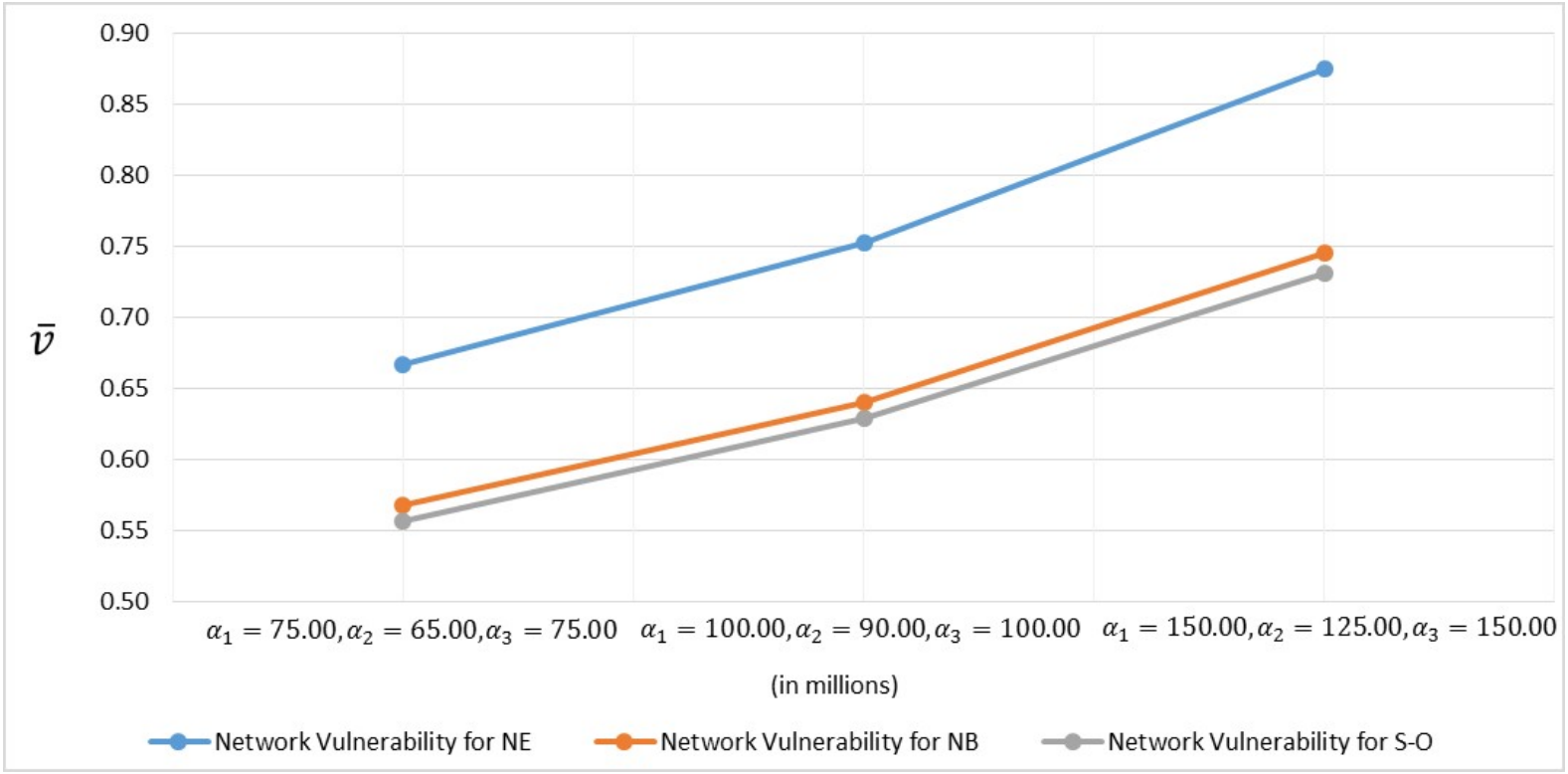


Figure: 2: Comparison of Network Vulnerability $\bar{v}$ for NE, NB, and S-O with Varying α_i Parameters with $D_1 = 25000.00$, $D_2 = 17200.80$ and $D_3 = 28000.50$

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**.
- NB yields enhanced network security for all cases as compared to 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**.
- NB yields enhanced network security for all cases as compared to NE.
- **Results support cooperation among firms** that are otherwise competitors. **NB is pragmatic given the emphasis on sharing cyber information**.

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**.
- NB yields enhanced network security for all cases as compared to NE.
- **Results support cooperation among firms** that are otherwise competitors. **NB is pragmatic given the emphasis on sharing cyber information**.
- **Nash Bargaining model is the most practical and beneficial** for firms, the network, and consumers alike in terms of security levels.

Thank you! [https://supernet.isenberg.umass.edu/]