Revista de Humanidades de Valparaíso Año 6, 2018, 2do semestre, No 12, págs. 115-140
Journal of Humanities of Valparaiso No 12 (2018): 115-140
eISSN 0719-4242

Hunting Hackers. A gift from the 'mute guest'*

Cazando hackers. Un regalo del 'convidado de piedra'

María Dolors Martínez-Cazalla**

Abstract

We can be hacked because *there are not indiscreet questions but there are imprudent answers*. The main aim of this paper is actually to learn how to create the best possible answers, the most prudent ones, in order to remain as safe as we can. That is what *Hunting Hackers* means: to think about what piece of information was relevant for the hacker and why that one in particular and not another. If we could preview our flaws then we would be able to keep our zone safer from hackers. In order to reach this objective, we will analyse how the cryptic language known as Russian Cards operates. This study does not intend to show how the cryptic language is broken into, but to take advantage of the learning gifted in knowing the flaw itself. It is precisely in the learning of the flaw that we can find the answer to what and why we may be hacked. In proportion to the amount of flaw information at our disposal, we will be able to hunt hackers: to stop them completely or, at least, to weaken a possible hacker attack.

Keywords: cryptic language; Russian Cards; dialogical semantics; safety information; anti-hacking protection.

---

* Recibido: 6/12/2018. Aceptado: 20/12/2018.

** Universidad de Sevilla, España. Email: madomartinezcazalla@gmail.com

Resumen

Podemos ser hackeados porque *no hay preguntas indiscretas sino respuestas imprudentes*. El objetivo principal de este artículo es aprender a crear las mejores respuestas posibles, las más prudentes, para permanecer los más seguros que podamos. Esto es lo que significa *cazando hackers*: pesar sobre qué pieza de información fue la relevante para el hacker y por qué lo fue esta y no, otra. Si podemos prever nuestras fisuras podremos mantener nuestra zona a salvo de los hackers. Con el fin de alcanzar este objetivo, analizaremos cómo funciona el lenguaje encriptado conocido como las Cartas Rusas. La intención de este estudio no es mostrar cómo romper el lenguaje encriptado, sino el provecho que hemos sacado del aprendizaje que nos ha regalado su punto débil en sí mismo. Precisamente es aprendiendo de este punto débil donde encontramos la respuesta al qué y al por qué podemos ser hackeados. En la medida en que dispongamos de esta información, estaremos preparados para cazar hackers: paralizar completamente o, al menos, debilitar un posible ataque.

Palabras clave: lenguaje cifrado; Cartas Rusas; semántica dialógica; información segura; protección anti-piratería.

1. Introduction

It is commonly accepted that is easier to attack than to defend. This belief is based on the idea that we need to wait for an attack before you know where weak spots are located. When we are working to create a safety zone we assume we have some flaws, but we do not know them beforehand. If we knew them, we would be aware of our position. Nevertheless, when we receive a hacker's attack we are somehow surprised, therefore we immediately start a defence mechanism. It is as if we needed to know the attack before we can decide on which defence weapons to use. While we are thinking, maybe already building a suitable shield for this attack, we are distracting attention from the rest of our system and new attacks may come in. In the end, we are completely infected. When this happens recurrently, it may be the right time to think differently. This paper aims to test this assumption.

Until now the defence paradigm has been that *the best defence is a good attack*. Besides, we always think of an active attack, even when we are usually thinking of defending: we could call that a *passive defence*, *i.e.* waiting for an attack and reacting then at the counterattack. We propose here to start thinking different lay because, if we want a different result, we should do something different. Doing the same we will only obtain the same known results. We propose thinking about an *active defence*, meaning a defence that can be produced before an attack has been received, and it is made out of a 'healthy' attitude that gains in security and safe time and material and human resources, turning then the best attack into a good defence.

In order to build an attack, the hacker needs some point of attachment, so they need to have some piece of truth, some information from our system. Otherwise any attack intended would have a very low chance of success. Hackers are always looking for the best result with the least effort, working as much as possible by choice and not randomly. Because the hacker works by means of making a choice, if they need a piece of information from our system, they will have access to us the moment we stay in a world accessible to them.

As *an image is worth a thousand words*, we will imagine the hacker as a 'mute guest', one who is sitting at the next table, looking bored while carefully listening to our talk during the coffee break. As we speak, we are always passing some information; this information is passed under a question-reply form. Questions create a limited set of possible replies, and when the chosen reply falls down, the set disappears and the reality has been created, a 'new' world has emerged. If this world is accessible for the 'mute guest' at some point, this point will become the attachment point and we can be sure we may be hacked. Therefore, *there are not indiscreet questions but there are imprudent answers*.

The main aim of this paper is actually to learn how to create the best possible answers, the most prudent ones, in order to remain as safe as we can. In order to reach this objective, we will analyse how the cryptic language known as Russian Cards operates. This study does not intend to show how the cryptic language was broken into, but to take advantage of the learning gifted in knowing the flaw itself. It is precisely in the learning of the flaw that we can find the answer to what and why we may be hacked. In proportion to

the amount of information at our disposal, we will be able to hunt hackers: to stop them completely or, at least, to weaken a hacker attack.

The way we propose to tackle this objective is, first, to analyse how the Russian Cards operates. We choose this cryptic language because it accurately illustrates why the 'mute guest' must be somebody in touch with our world, the world we want to keep safe in order to guarantee our own security. Second, we can learn two lessons from the analysis of the 'mute guest' figure, as explained below. Finally, we will discover the gift received from the behaviour of the 'mute guest'.

2. Cryptic language: Russian Cards. How are they operating?

This section deals with a cryptic language: the Russian Cards. The original problem was proposed at the Moscow Mathematics Olympiad in 2000:

> **Level C. Problem 6.** Seven cards were drawn from a deck, shown to everybody, and shuffled. Then Greg and Linda were given three cards each, and the remaining card was either (a) hidden or (b) given to Pat. Greg and Linda take turns announcing information about their cards. Are they able to ultimately reveal their cards to each other in such a way that Pat cannot deduce the location of any card he doesn't see? (No special code was set up in advance; all announcements are in "plain text".) (Fedorov et al., 2011, 5)

Thus, we are inside a typical framework for a Dynamic Epistemic Logic (hereunder, DEL). The progress of knowledge depends on the public announcements (cf. Van Ditmarsch et al., 2008, 104-107) made by the knowledge subjects involved —in our case: Greg, Linda and Pat—. We can say Greg and Linda are active knowledge subjects and Pat is just a passive subject, like a 'mute guest'.

Is the 'mute guest' a true passive subject or could she be a 'hacker in disguise'? The aim of this section is to answer this question. We will analyse the Russian Cards from the dialogical semantics because our interest is to find out what is happening in Pat's mind, what is Pat thinking when she is listening to announcements from Greg and Linda (as you can see, we are not using at the moment the word knowledge for Pat because the problem states: *Greg and*

Linda can exchange information about the hands they hold without Pat being able to deduce the owner of any card other than her own). So, our interest is in the field of semantics, in the meaning of what is being said. Only at the end of this reasoning we will get to know what has changed in Pat's knowledge.

For this analysis we will take the Russian Cards problem developed by van Ditmarsch (Van Ditmarsch, van der Hoek & Kooi 2008, 97-104 et 108). First, we will tackle its dialogical semantics form for the general case. Then we will be ready to think what is happening in Pat's mind in each case shown. Note that in the van Ditmarsch's Russian Cards the names of the characters have been changed: Greg is Ann (a), Linda is Bill (b) and Pat becomes Cath (c).

A dialogical semantics[1] for the Russian Cards[2]

1. Mathematical rules for the Russian Cards:

1.1. Characteristics of the game:

- We have three players: a; b; c.
- We have a stack with seven different cards. They are numbered: 0; 1; 2; 3; 4; 5; 6.
  C={0,1,2,3,4,5,6}
- The card deal for player 'a' and for player 'b' is the same: three cards each; player 'c' gets only one card.
- The language assumes expressions in the form gR(m,n,p), that should be interpreted as player g has the cards m; n; p. More precisely:
  aR(m, n, p); bR(m', n', p'); cR(m'')
  where m; n; p; m'; n'; p'; m" are (different) numbers from 0 to 6.

[1] Cf. for rules of intuitionistic dialogical semantics —points: 2, 3, 4 and 5 of this section— Rahman & Clerbout (2015) and Redmond & Fontaine (2011).

[2] Fulfilling correction and completeness within the Dialogical Epistemic Multi Agent Logic (DEMAL) framework. Cf. Magnier 2013, 80-98.

In order to simplify the notation, we will follow the convention used by van Ditmarsch, van der Hoek & Kooi (2008), from whom expressions of the form aR(m, n, p) are taken: mnpa and so on.

1.2. Objective of the game:

The game has only one objective and it consists of two parts:

Part 1: players 'a' and 'b' interchange information about the cards they hold.

Part 2: after this sharing, player 'c' must be still ignorant, or in other words, he still knows only his own card and does not know who has what.

Hence the objective of the game can be rendered with the following expression $[K_a(mnp_a) \wedge K_a(m'n'p'_b)] \wedge [K_b(m'n'p'_b) \wedge K_b(mnp_a)] \wedge [K_c(m''_c) \wedge \sim K_c(mnp_a) \wedge \sim K_c(m'n'p'_b)]$ that reads.

1.3. Knowledge stage or terms of the game:

- The 3 players (a; b; c) know that 7 cards have been dealt. They are not duplicated and they are numbered 0 to 6: C={0,1, …, 6}
- The deal has been: $C_{(a)}{}^{3}{}_{7} * C_{(b)}{}^{3}{}_{4} * C_{(c)}{}^{1}{}_{1} = aR({}^{3}{}_{7}); bR({}^{3}{}_{4}); cR({}^{1}{}_{1}) = 140$ deals are possible.
- Player 'a' and player 'b' have to let each other know the cards they hold without discovering them to player 'c'. Player 'c' has to remain ignorant about who has what after their announcements (in accordance with the objective of the game —previous section: 1.2.— and inside the framework of the logic of the public announcements —next section: 1.4.—).
- At first, every player knows only his own cards.
- After the deal the cards distribution has been: 012_a; 345_b; 6_c.

2. Particle rules:

Announcement structure	Attack	Defence
$!\alpha\wedge\beta$ The attacker chooses the defence	$?L_{\wedge}$	$!\alpha$
	$?R_{\wedge}$	$!\beta$
$!\alpha\vee\beta$ The defender chooses the defence	$?_{\vee}$	$!\alpha$
		$!\beta$
$!\alpha\rightarrow\beta$	$!\alpha$ (α is assumed to occur)	$!\beta$
$!\neg\alpha$	$!\alpha$	----------
$!\forall_x A_x$	$?_k$ (k is chosen by the attacker)	$!A_k$
$!\exists_x A_x$	$?\exists$ (could you show me one, please?)	$!A_k$ (k is chosen by the defender)
$!\Box A_{ci}$	$?_{cj}$ <ciRcj> (cj is chosen by the attacker)	$!A_{cj}$
$!\Diamond A_{ci}$	$?\Diamond$ (could you show me a case, please?)	!Acj <ciRcj> (cj is chosen by the defender)

Note: For '□' and '◊', it will be the same in all the cases where there is a modal operator: alethic, deontic, epistemic, doxastic, temporal or a combination of them.

3. Structural rules for a game played inside the intuitionistic logic:

- Player 'c' always remains as 'mute guest'.
- The game starts with an assertion from player 'a'.
- By rotating turns, player 'a' first, then 'b', and again 'a' and 'b', make a public announcement, either as an assertion or as a question.
- Each announcement —assertion or question— must be true.
- Each announcement produces a new 'engagement' that adds to the previous ones, making an 'engagement' chain. No player can avoid his 'engagement chain'.
- No player can repeat an argument already attacked. If an argument is repeated it will be because the player arrives to the same argument through a different way (*i.e.*: from another hypothesis).
- Each announcement has to have a reply. It is not possible to leave an announcement without reply. At the end of the game each attack must be completed with its defence, unless:
  - The attack has been against a negative sentence. Then, no reply, no defence is possible.

    i.e.: Cf. Rahman & Clerbout, 2015, 68.

	O			**P**	
				! $A_{\vee}\neg A$	0
1	? $[A_{\vee}\neg A]$	0		! $\neg A$	2
3	! A	2		--	

O Wins

  - The attack has been a double negative sentence. Negative sentences can only be attacked one at a time because, as just seen two points before, no player can avoid his 'engagement chain', so no player can say !A when he has already said !$\neg A$. Therefore, faced with attacks against double negative sentences, a double attack will not be possible (being A an elementary proposition).

    i.e.: Cf. Rahman & Clerbout, 2015, 69.

	O			**P**	
				! ¬ ¬*A*→*A*	0
1	! ¬ ¬*A*	0			
	--		1	! ¬*A*	2
3	! *A*	2		--	

O Wins

- The attack has been an elementary proposition and the respondent does not have the possibility to reply the same elementary proposition.

  i.e.: Cf. Rahman & Clerbout, 2015, 66.

	O			**P**	
				! *Oa*→*Ob*	0
1	! *Oa*	0		--	2

O Wins

- *The best defence is a good attack*. If we can choose between attacking and defending, in most instances we should attack first.
- The game ends when 'a' knows b's deal and *vice versa*, and 'c' remains ignorant.

4. Formalisation for the general case:

Case 3.1.

OPPONENT (b)			PROPONENT (a)		
	HYPOTHESIS		**THESIS**		
H1	$g \neq g' \neq c$; $g,g' \in \{a,b\}$		$!(012_a \vee 012_b) \rightarrow [(012_a \vee 012_b) \wedge (345_a \vee \vee 345_b)]$		0
H2	$C=\{0,1,2,3,4,5,6\}$				
H3	$mnp_g \rightarrow (\sim mnp_{g'} \vee \sim m'n'm''_{g'} \vee \vee \sim n'p'm''_{g'} \vee \sim m'p'm''_{g'} \vee m'n'p'_{g'})$				
H4	$\{m \neq n \neq p \neq m' \neq n' \neq p' \neq m''\} \in C$				
H5	$m'' \in \{c\}$ then m''_c				
1	$!(012_a \vee 012_b)$	0		$![(012_a \vee 012_b) \wedge (345_a \vee 345_b)]$	4
3	$!012_a$		1	$?\vee$	2
5	$?L\wedge$	4		$!(012_a \vee 012_b)$	6
7	$?\vee$	6		$!012_a$	8
9	$?R\wedge$	4		$!(345_a \vee 345_b)$	10
11	$?\vee$	10		$!345_b$	20
13	$!012_g \rightarrow (\sim 012_g \vee \sim 346_g \vee \sim 456_g \vee \vee \sim 356_g \vee 345_{g'})$		(3) H3	!m/0;n/1;p/2;m'/3;n'/4;p'/5;m''/6	12
15	$!012_a \rightarrow (\sim 012_b \vee \sim 346_b \vee \sim 456_b \vee \vee \sim 356_b \vee 345_b)$		(3) H3	!g/a;g'/b	14
17	$!\sim 012_b \vee \sim 346_b \vee \sim 456_b \vee \sim 356_b \vee 345_b$		15	$!012_a$	16
19	$!345_b$		(H5) 17	$?\wedge$	18

Summary for case 3.1: a holds 012 and b holds 345.

OR:

Case 3.2.

OPPONENT (b)			PROPONENT (a)		
	HYPOTHESIS		**THESIS**		
H1	g≠g'≠c; g,g'ϵ{a,b}		$!(012_a \vee 012_b) \rightarrow [(012_a \vee 012_b) \wedge (345_a \vee \vee 345_b)]$		0
H2	C={0,1,2,3,4,5,6}				
H3	$mnp_g \rightarrow (\sim mnp_{g'} \vee \sim m'n'm''_{g'} \vee \vee \sim n'p'm''_{g'} \vee \sim m'p'm''_{g'} \vee m'n'p'_{g'})$				
H4	{m≠n≠p≠m'≠n'≠p'≠m"}ϵC				
H5	m"ϵ{c} then m''_c				
1	$!(012_a \vee 012_b)$	0		![(012a∨012b)∧(345a∨345b)]	4
3	$!012_b$		1	?∨	2
5	?L∧	4		$!(012_a \vee 012_b)$	6
7	?∨	6		$!012_b$	8
9	?R∧	4		$!(345_a \vee 345_b)$	10
11	?∨	10		$!345_a$	20
13	$!012_{g'} \rightarrow (\sim 012_g \vee \sim 346_g \vee \sim 456_g \vee \vee \sim 356_g \vee 345_g)$		(3) H3	!m/0;n/1;p/2;m'/3;n'/4;p'/5;m"/6	12
15	$!012_b \rightarrow (\sim 012_a \vee \sim 346_a \vee \sim 456_a \vee \vee \sim 356_a \vee 345_a)$		(3) H3	!g/a;g'/b	14
17	$!\sim 012_a \vee \sim 346_a \vee \sim 456_a \vee \sim 356_a \vee 345_a$		15	$!012_b$	16
19	$!345_a$		(H5) 17	?∧	18

Summary for case 3.2: a holds 345 and b holds 012.

5. Interpretation keys:

- External columns contain the intervention order number, that is, the number of the game moves.
- The number of move that is being attacked is placed in the internal double column. If the number is placed on the left, that means that the opponent is attacking a move from the proponent [e.g.: move 1 (opponent) is attacking move 0 (proponent)]. If the number is placed on the right, then the proponent is attacking a move from the opponent [e.g.: move 2 (proponent) is attacking move 1 (opponent)]. Numbers in brackets above the attacked move number mean: 'as you said at move x or as you said at hypothesis x, I can attack you as I am doing now' [e.g.: move 14 (proponent) is attacking move 13 (opponent), his attack is based on Hypothesis 1 (H1)].
- The central columns contain announcements: centre left are the opponent's announcements and centre right are the proponent's.
- Each announcement is preceded by a sign:

  '!': This means that the announcement is an assertion.

  Assertions could be the pragmatic form of an attack and also of a defence.

  '?': This means that the announcement is not a 'proper' one; it is a question about a previous announcement.

  Question could be the pragmatic form of an attack and also of a defence.

- Each row comprises 6 boxes (from left to right):

  1. box for the number of the opponent's move.
  2. box for the opponent's announcement (attack or defence under the form of an assertion or a question).
  3. box for the number of move attacked by the opponent to the proponent —if this is the case.
  4. box for the number of move attacked by the proponent to the opponent —if this is the case.
  5. box for the proponent's announcement (attack or defence under the form of an assertion or a question).

6. box for the number of the proponent's move.

- Box 2 and box 5 must be coordinated: if box 2 is an attack then box 5 must be its defence (and does not necessarily have to be the next move). Thus, we will hold an attack and its defence on the same row and it is not relevant if the defence is the next move or if it happens many moves after the attack (e.g.: move 11 is an attack by the opponent to move 10 of the proponent. This attack is defended —replayed— on proponent's move 20). Therefore, each new attack must be placed in a new row in order to keep its defence box empty.

Once we have dealt with the semantics for the general case, we should tackle the cases proposed by van Ditmarsch (2008) one by one, following the convention used by van Ditmarsch (*i.e.*: Exercise 4.72, etc.). This will help us answer the question we proposed: is the 'mute guest' a true passive subject or could be he a 'hacker in disguise'? To accomplish this we are not going to formalise each case in a dialogical semantics form. We consider that we do not need 'to repeat' it for each case, once we know how dialogical semantics work, because our interest is in the 'hidden column', the one for the 'mute guest', Cath (c). So, we will hear the announcements as 'c' would listen to them and we will imagine what kind of reflections would be happening in her mind.

> **Exercise 4.72 (A five hand solution):** Assume deal of cards 012.345.6. Show that the following is a solution: Anne announces: "I have one of {012, 034, 056, 135, 246}" and Bill announces "Cath has card 6". (Van Ditmarsch, 2008, 103)

Bill (b) (opponent)		**Ann (a) (proponent)**		**Cath (c) ('mute guest')**
2	!6c	$!012_a \vee 034_a \vee 056_a \vee 135_a \vee 246_a$	1	???

What is 'c' thinking after a's and b's announcements?

1. How did 'b' know I have card 6?
2. If 'b' said 6 and not another out of the four possible cards, those ones that 'b' does not have must be because.

2.1. In triads announced by a where card 6 is there must be also at least one of b's cards.

2.2. As each triad must guarantee the safety of the announcement, then no one can be inside the 'true zone' of another player (you can only have total control of your 'true zone'). To be sure, the only possible solution is to include *only one* proper card number of the announcer in each one of the triads.

2.3. In the triads where 6 is, there is also a card from 'b' (as seen just above: 2.1.). Thanks to this 'b' knows these triads as not a's triads. The triads contain also one of a's cards to guarantee the safety of the announcement (as seen at 2.2.).

2.4. Therefore, if 'b' announces, "Cath has card 6", a does not have a triad where the 6 is.

3. So 'c' removes these triads from a's announcement, and the result is a 'new' a's announcement: $!012_a \vee 034_a \vee 135_a$

4. 'c' asks herself what is a's hand. To answer, she will be doing the following reasoning:

4.1. In the triads where 6 is (056; 246), there is also one card of 'a' and another of 'b', so:

a = 0; 2	then	b = 5; 4
a = 5; 4	then	b = 0; 2
a = 0; 4	then	b = 2; 5
a = 2; 5	then	b = 0; 4

4.2. Next step in c's reasoning is comparing these binomials to the three remaining triads (as seen in 3.): $012_a \vee 034_a \vee 135_a$. The result is that either a holds 012 or 034, therefore a holds 0 and b must hold either 25 or 54, so b holds 5.

4.3. Now 'c' knows two of a's triads for sure: $012_a \vee 034_a$ and one (135_a) like a 'doubt', we may say, because there is no light coming on that one after comparing it to the triads including 6.

4.3. Now, 'c' compares the possible a's binomial to the triads containing card 6 (056; 246), looking for more information, *but nothing new is coming up*.

012 to 056: as 'b' said c holds 6, and 'c' knows already 'b' holds 5 and 'a' holds 0.

034 to 056: This is the same case as above.

012 to 246: as 'b' said 'c' holds 6, and 'c' knows a holds 0, and 0 should be together with 2 or with 4. For this case 'c' would think 'a' holds 2 and 'b' holds 4.

034 to 246: This is the opposite of the former case, here 'c' would think 'a' holds 4 and 'b' holds 2. In this case 'c' would be in a GREAT mistake. So from here we can conclude that this part of the reasoning (4.3.) is not reliable. Therefore the reasoning of 'c' should always conclude at the previous step (4.2.).

c's most likely final state of knowledge is:

$012_a \vee 034_a$

a = 0; 2 then b = 5; 4. Therefore 012_a and 543_b

or

a = 0; 4 then b = 2; 5. Therefore 034_a and 251_b

As the deal has been: $C_{(a)}{}^{3}{}_{7} * C(b)^{3}{}_{4} * C(c)^{1}{}_{1} = aR(^{3}{}_{7}); bR(^{3}{}_{4}); cR(^{1}{}_{1}) = 140$ deals are possible. At the beginning, 'c' knows she holds 6, so the possible deals are only the ones where 'c' holds 6, therefore there are 20 possible deals: $C_{(a)}{}^{3}{}_{6} * C_{(b)}{}^{3}{}_{3} = aR(^{3}{}_{6}); bR(^{3}{}_{3}) = 20$. In fact, Cath is only hesitating between two possible deals $[(012_a \wedge 543_b) \vee (034_a \wedge 251_b)]$, thus 'c' knows 18 deals that are not possible. If 20 unknown deals mean 100% of c's ignorance, then 2 unknown deals will be 10% of c's ignorance. In this case, Cath has reached a knowledge of 90% according to the deals and 33.3333% knowledge about the composition of each deal ('c' knows one card from 'a' (0) and one from 'b' (5)).

Total c's knowledge is 93.3333% Total c's ignorance is 6.6667%

If we are including the 'doubt' (135_a) then c's final state of knowledge will be:

$$012_a \vee 034_a \vee 135_a$$

Total c's knowledge is 85% Total c's ignorance is 15%

In this case 'c' cannot reach more knowledge because no card is common for all three of a's possible deals.

Exercise 4.73 (A six hand solution): Assume deal of cards 012.345.6. Show that the following is a solution: Anne announces: "I have one of {012, 034, 056, 135, 146, 236}" and Bill announces "Cath has card 6". (Van Ditmarsch, 2008, 103)

Bill (b) (opponent)		**Ann (a) (proponent)**		**Cath (c) ('mute guest')**
2	!6c	$!012_a \vee 034_a \vee 056_a \vee 135_a \vee 146_a \vee 236_a$	1	???

What is c thinking after a's and b's announcements?

1. How did 'b' know I have card 6?
2. If 'b' said 6 and not another out of the four possible cards, those ones 'b' does not have must be because:
   - 2.1. In triads announced by a, where card 6 is, there is also at least one of b's cards.
   - 2.2. As each triad must guarantee the safety of the announcement, then no one can be inside the 'true zone' of another player (you can only have total control of your own 'true zone'). To be sure, the only possible solution is to include *only one* proper card number of the announcer in each one of the triads.
   - 2.3. In the triads where 6 is, there is also a card from 'b' (as seen just above: 2.1.). Thanks to this b knows these triads as not a's triads. The triads contain also one of a's cards to guarantee the safety of the announcement (as seen at 2.2.).
   - 2.4. Therefore, if 'b' announces, "Cath has card 6", a does not have a triad where 6 is.

3. So 'c' removes these triads from a's announcement, and the result is a 'new' a's announcement: $!012_a \vee 034_a \vee 135_a$
4. 'c' asks herself what is a's hand? To answer, she will be doing the following reasoning:

4.1. In the triads where 6 is (056; 146; 236), there is also one card of 'a' and another of 'b', so:

a = 0; 1; 2	then	b = 5; 4; 3
a = 5; 4; 3	then	b = 0; 1; 2
a = 0; 1; 3	then	b = 5; 4; 2
a = 5; 4; 2	then	b = 0; 1; 3
a = 0; 3; 4	then	b = 1; 2; 5
a = 5; 1; 2	then	b = 0; 4; 3
a = 0; 4; 2	then	b = 1; 3; 5
a = 1; 3; 5	then	b = 0; 4; 2

4.2. Next step in c's reasoning is comparing the above triads (4.1.) to the three remaining triads (as seen in 3.): $012_a \vee 034_a \vee 135_a$. The result is that every one of them could be possible because all are compatible with the condition to include one card from 'a' + one card from 'b' + 6.

c's final state of knowledge is:

$012_a \vee 034_a \vee 135_a$

a = 0; 1; 2	then	b = 5; 4; 3.	Therefore 012_a and 543_b
or			
a = 0; 3; 4	then	b = 1; 2; 5.	Therefore 034_a and 125_b
or			
a = 5; 1; 3	then	b = 0; 4; 2.	Therefore 135_a and 042_b

As the deal has been: $C_{(a)}{}^{3}{}_{7} * C_{(b)}{}^{3}{}_{4} * C_{(c)}{}^{1}{}_{1} = aR(^{3}_{7}); bR(^{3}_{4}); cR(^{1}_{1})$=140 deals are possible. At the beginning, 'c' knows she holds 6, so now the possible deals are only the ones where 'c' holds 6, therefore there are 20 possible deals: $C^{(a)3}{}_{6} * C_{(b)}{}^{3}{}_{3} = aR(^{3}_{6}); bR(^{3}_{3})$=20. In fact, Cath is only hesitating between three possible deals $[(012_a \wedge 543_b) \vee (034_a \wedge 125_b) \vee (135_a \wedge 042_b)]$, thus 'c' knows

17 deals are not possible. If 20 unknown deals mean 100% of c's ignorance, then 3 unknown deals will be 15% of c's ignorance. In this case, Cath has reached knowledge of 85%. In this case 'c' cannot reach more knowledge because no card is common for all three of a's possible deals.

Total c's knowledge is 85% Total c's ignorance is 15%

Exercise 4.74 (A seven hand solution): Assume deal of cards 012.345.6. Show that the following is a solution: Anne announces: "I have one of {012, 034, 056, 135, 146, 236, 245}" and Bill announces "Cath has card 6". (Van Ditmarsch, 2008, 103)

Bill (b) (opponent)		**Ann (a) (proponent)**		**Cath (c) ('mute guest')**
2	!6c	$!012_a \vee 034_a \vee 056_a \vee 135_a \vee 146_a \vee 236_a \vee 245_a$	1	???

What is 'c' thinking after a's and b's announcements?

Now, after doing the previous exercises, c has reached a quite refined method. She knows the procedure is:

1. To take off the triads where her card, 6, is. Then, for this case, the 'new' a's announcement would be: $!012_a \vee 034_a \vee 135_a \vee 245_a$
2. She also knows that it is not necessary to do step 4.3. That has been done during the first exercise and it was decided not to do it again because it was considered not to be a reliable way.
3. Once she knows how the 'new' a's announcement looks (an announcement that will not contain her card in any triad), she needs to compare the possible resulting (a-b)'s deals to the announced triads containing 6, her card.

a-b possible pairs, according to a's announcement are:

a = 0; 1; 2 then b = 3; 4; 5
a = 0; 3; 4 then b = 1; 2; 5
a = 1; 3; 5 then b = 0; 2; 4
a = 2; 4; 5 then b = 0; 1; 3

Final c's state of knowledge is: after comparing a's possible deals to the triads including 6 (056; 146; 236) no new knowledge is gained. So:

$012_a \vee 034_a \vee 135_a \vee 245_a$

a = 0; 1; 2 then b = 5; 4; 3. Therefore 012_a and 543_b

or

a = 0; 3; 4 then b = 1; 2; 5. Therefore 034_a and 125_b

or

a = 5; 1; 3 then b = 0; 4; 2. Therefore 135_a and 042_b

or

a = 2; 4; 5 then b = 0; 1; 3. Therefore 135_a and 042_b

As the deal has been: $C_{(a)}{}^{3}{}_{7} * C_{(b)}{}^{3}{}_{4} * C_{(c)}{}^{1}{}_{1} = aR(^{3}_{7})$; $bR(^{3}_{4})$; $cR(^{1}_{1})$=140 deals are possible. At the beginning, 'c' knows she holds 6, so now the only possible deals are the ones where 'c' holds 6, therefore there are 20 possible deals: $C_{(a)}{}^{3}{}_{6} * C_{(b)}{}^{3}{}_{3} = aR_{(36)}$; $bR(^{3}_{3})$=20. However, Cath is only hesitating between four possible deals $[(012_a \wedge 543_b) \vee (135_a \wedge 042_b)]$, thus 'c' knows 16 deals are not possible. If 20 unknown deals mean 100% of c's ignorance, then 4 unknown deals will be 20% of c's ignorance. In this case, Cath has reached knowledge of 80%. In this case 'c' cannot reach more knowledge because no card is common for all four of a's possible deals.

Total c's knowledge is 80% Total c's ignorance is 20%

At this point we can assume we are ready to deal with the question regarding the 'mute guest' because, even if we would continue with the rest of the proposed exercises by van Ditmarsch (2008), we think they are no relevant any more, now that we know the method, so its application will be similar every time. Even increasing the difficulty of the algorithm, that is, increasing the number of cards while maintaining the proportion on the deal for 'a' and 'b' and 'c' always one (3:3:1; 4:4:1; …; n:n:1) or increasing the number of cads for all of them, maintaining the proportion always (3:3:1; 4:4:2; …; n:n:n-2), the method would be applied in the same way (so, one of the announced matrices must be the proponent's deal and the rest must contain *only one* element from the proponent's deal, as said in point 2.2. of the exercises) only the rank of the announced matrices will change (it must always be the

rank of deal for 'a' and 'b') together the number of announced matrices needed to keep announcements safe.

Thus, the question would be whether the 'mute guest' is a true passive subject or a 'hacker in disguise'. We think the answer is quite clear. As far as the 'mute guest' is really mute but not deaf, we cannot be so arrogant as to think that the 'mute guest' is not thinking about what they are hearing. We can never assert that they are just hearing and not listening. If they are listening, they could be thinking about it. If they are thinking, they will then reach some amount of knowledge. So, a 'mute guest' is not a 'passive' subject because of being mute, they can be 'passive' (hearing and not listening, then not thinking) or not, that is their choice, nothing else.

Therefore, the chance to have a 'hacker in disguise' 'hidden' as the 'mute guest' could be quite high because: the hacker's performance is just to be 'hidden'; to be 'mute' while others are talking; listening and not just hearing; gathering information from the others during the information exchanges; thinking why something is said and not something else and/or in another words, where the possible flaws could be ('flaws' meaning 'information leaks', the information which is said —including silence— in an unsafe form) and then, if flaws are found, they could decide to start the attack or not: professional attacks are not done at random, they are done with some degree of previous knowledge, and knowledge about others is only obtained from themselves. The hacker's job is no other than catching the 'leaking information' and to take advantage of it, using it to conduct a more effective attack. We must be careful, since even when information is passed in a safe form, we cannot be sure if some information is 'leaking'. Information is information anyway; even silence provides information, because silence encodes usually a finite number of replies to the question that triggered the silence. Thus, a 'mute guest' is not the best guest when you want to pass information without being recorded.

Anyway, the existence of 'mute guests' enhances the argumentative capacities between the interlocutors, they are required to do their announcements as correctly as possible (both in quality and safety). A 'mute guest' could be the best coach for conversational partners. In the next section we will refer to two relevant lessons learned from the 'mute guest' addressed at preserving safety in our world.

3. Two lessons from the 'mute guest'

As it has been shown just before, being coached as an information subject in the presence of a 'mute guest', a 'potential hacker', helps us know what and why they are thinking based on our announced arguments; therefore we can enhance our way of communicating, improve the structure of our announcements —their quality and safety— from the point of view of a syntactic pattern where the content is expressed. A 'potential hacker' is the best mirror we can have; by observing them we can learn the most about the potential flaws we have in the piece of information we are preparing to pass, because a hacker is nothing but the worst opponent.

The two great lessons from the 'mute guest' are the following:

1. The potential hacker starts thinking 'hard' against us when we directly trespass their 'true zone' (*i.e.*: Bill announces: "Cath has card 6"). When anybody feels their 'true zone' directly trespassed, the natural reaction is to think: why do they say that? How can they know? Everybody's 'true zone' is the core of their 'comfort zone', and nobody likes it to be trespassed, and much less so with a direct allusion. When somebody feels overstepped, they feel in danger. Then there are only two possible reactions: either fighting back against this invasion or transforming our unintended direct attack into the hardest counterattack we can expect because, as we have seen in the previous section, announcing our opponent's truth is the least safe we can do, it is the most revealing action we can make, it shows much more of our 'true zone' than talking about our proper true, like Ann did in her announcement.

   > **Thus, first lesson:** the 'mute guest' says: 'do not touch me, please, or at least not shamelessly'. That is, if you want to remain safe, when passing a piece of information you must be aware that you are only speaking the truth because a lie may be the hacker's truth.

2. His second lesson is in correspondence with the previous one. Now we know that it is not safe to trespass our opponent's 'true zone' directly, then how will we be able to attack and remain safe? The best plausible way would be to create our replies to the proponent's an-

nouncements is to follow a similar pattern to the one that we would use to reply a partner in the presence of a hacker. The question is how Bill could answer Ann and not increase Cath's already acquired knowledge (from Ann's announcement). The way to do it is just the one we use naturally, when we give information not to be understood by a third person: we usually reply repeating the same pattern used before, like going along with the same —but it is not quite the same— (*i.e.*: Ann announces: "I have one of {012, 034, 056, 135, 146, 236, 245}", then Bill's reply could be just the inverse of the part of announcement already 'caught' by Cath. Thus, Bill's reply could be: 'I have one of {345, 543, 056, 042, 146, 236, 013}'). This adds nothing to Cath's knowledge:

a = 0; 1; 2 then b = 5; 4; 3. Therefore 012_a and 543_b

or

a = 0; 3; 4 then b = 1; 2; 5. Therefore 034_a and 125_b

or

a = 5; 1; 3 then b = 0; 4; 2. Therefore 135_a and 042_b

or

a = 2; 4; 5 then b = 0; 1; 3. Therefore 135_a and 042_b

and

$[K_a(mnp_a)\wedge K_a(m'n'p'_b)]\wedge[K_b(m'n'p'_b)\wedge K_b(mnp_a)]\wedge[K_c(m''_c)\wedge\sim K_c(mnp_a)\wedge\sim K_c(m'n'p'_b)]$

This is not exactly so, however Cath has no more knowledge after Ann's announcement.

Thus, this is the second lesson: if you want to remain safe from the hacker's attack, when you are replying to a piece of information, you must create a new piece of information in the same pattern used before.

We cannot be so naïve as to believe that we will never touch the 'true zone'/'comfort zone' of a possible hacker. We should not undervalue hackers, and we should prepare the information transmission as if it were a struggle against an intelligent hacker; by doing so, we will do the best we possibly can to stay safe.

4. Conclusion: Hunting Hackers. A gift from the 'mute guest'

As we said at the beginning of this paper, the main aim of this study is actually to learn how to create the best possible answers, the most prudent ones, in order to remain as safe as we can. And we can state we have to do so by 'wrapping' the information in a kind of syntactic pattern as secure as possible; usually the better we 'wrap' the question, the better the answer we will obtain. But, sometimes, a question is really safe and its answer is completely unsafe —as was Bill's—, that is, imprudent (we can find the same idea in Petruzzi, 2012, 29). Thus, the gift is precisely the Russian Cards' flaw: the way in which Bill is replaying; he does not 'wrap' his answer securely; he does not 'wrap' his reply safely at all. Here, weakness has been converted into strength, a real gift. This is the meaning of *active defence*: finding the strength inside the weakness. Therefore, inside the weakness of the dialogue between Ann and Bill, Cath shows us how to convert a weak reply into strength, how to build prudent replies to stay as safe as possible. This is Cath's gift.

In any case, it is always better to use the dialogical semantical form that is the most favourable for us. As proponents, we will be able to choose our defence —*active defence*— (structures in green in the table below) and do not give to the possible hacker —opponent— weapons to be attacked with (structures in red in the table below).

Dialogical semantical form

Announcement structure	Attack	Defence
$!\alpha\wedge\beta$ The attacker chooses the defence	$?L_{\wedge}$	$!\alpha$
	$?R_{\wedge}$	$!\beta$
$!\alpha\vee\beta$ The defender chooses the defence	$?_{\vee}$	$!\alpha$
		$!\beta$
$!\alpha\rightarrow\beta$	$!\alpha$ (α is assumed to occur)	$!\beta$
$!\neg\alpha$	$!\alpha$	----------
$!\forall_x A_x$	$?_k$ (k is chosen by the attacker)	$!A_k$
$!\exists_x A_x$	$?\exists$ (could you show me one, please?)	$!A_k$ (k is chosen by the defender)
$!\Box A_{ci}$	$?_{cj}$ <ciRcj> (cj is chosen by the attacker)	$!A_{cj}$
$!\Diamond A_{ci}$	$?\Diamond$ (could you show me a case, please?)	!Acj <ciRcj> (cj is chosen by the defender)

Note: For '□' and '◊', it will be the same in all the cases where there is a modal operator: alethic, deontic, epistemic, doxastic, temporal or a combination of them.

As a rule it can be said that it is better to make announcements under a disjunctive form, a particular form, a possible form, or a combination of them. Moreover, in the particular case of a conditional announcement (no literal

expression: no literal antecedent and no literal consequent, understanding 'literal' as an elementary proposition or its negative form), the best choice is to use:

- the consequent under one of these forms mentioned just above, because then we will receive a 'favourable' attack; and
- the antecedent under an assertion —elementary proposition—, a conjunctive form, a universal form, a necessary form or a combination of them, because then we will be able to fight back (once our conditional is attacked). Finally, it should always be kept in mind that negative assertions are automatically interpreted as positive, and they may have consequences opposite to what should be expected (cf. CoE, 2014, 69; Petruzzi, 2012, 77). Be extremely careful about this because no defence is possible after such an assertion has been said.

In the end, we are very grateful to Cath, the 'mute guest' and our hacker, for teaching us how to hunt her.

References

CoE. Centre of Excellence (2014). *NLP Practitioner Course*. Manchester: CoE.

Fedorov, Roman, et al. (ed.) (2011). *Moscow Mathematical Olympiads, 2000-2005*. Providence, Rhode Island: Mathematical Sciences Research Institute & American Mathematical Society.

Lorenz, Kuno and Lorenzen, Paul (1978). *Dialogische Logik*. Darmstadt: Wissenschaftliche Buchgesellschaft.

Magnier, Sébastien (2013). Considérations dialogiques autour de la dynamique épistémique et de la notion de condition dans le droit (PhD thesis). University of Lille-3, Villeneuve d'Ascq, France.

Petruzzi, Jimmy (2012). *Going for Gold*. Peterborough: FastPrint Publishing.

Rahman, Shahid and Clerbout, Nicolas (2015). *Las Raíces Dialógicas de la Teoría Constructiva de Tipos*. Retrieved from https://halshs.archives-ouvertes.fr/halshs-01238172/document, checked on September 14, 2018.

Redmond, Juan and Fontaine, Matthieu (2011). *How to Play Dialogues. An Introduction to Dialogical Logic*. Dialogues Series, Vol. 1. London: College Publications.

Van Ditmarsch, Hans, van der Hoek, Wiebe and Kooi, Barteld (2008). *Dynamic Epistemic Logic*. Synthese Library Series, Vol. 337. Dordrecht: Springer.