Yura: Relaciones internacionales

Departamento de Ciencias Económicas, Administrativas y de Comercio

Revista electrónica ISSN: 1390-938x

N° 22: Abril - junio 2020

El planeamiento estratégico del ciberataque de Rusia a Estonia: aproximaciones desde teoría de juegos pp. 1 - 31

Rubbi, Lautaro Nahuel y Barlaro Rovati, Bruna

Universidad Argentina de la Empresa (UADE)

Buenos Aires - Argentina

Lima 775, C1073 CABA.

lrubbi@uade.edu.ar - bbarlarorovati@uade.edu.ar

El planeamiento estratégico del ciberataque de Rusia a Estonia: aproximaciones desde teoría de juegos

Rubbi, Lautaro Nahuel y Barlaro Rovati, Bruna
Universidad Argentina de la Empresa (UADE)
lrubbi@uade.edu.ar - bbarlarorovati@uade.edu.ar

Resumen

En 2007 Estonia sufrió una serie de ciberataques disruptivos por parte de Rusia que ubicaron al ciberespacio como un nuevo campo de batalla. Desde la academia se buscaron dar muchas explicaciones sobre por qué Rusia desarrolló este ataque. No obstante, pocos análisis indagaron sobre la decisión de realizar un ciberataque por sobre otras opciones posibles, la vías diplomática, las sanciones económicas o los actos de índole militar. Este trabajo pretende analizar las causas por las que Rusia optó por tal medio y no por otro, explicado desde la perspectiva hipotético-deductiva de la teoría de juegos. Asimismo, se propone estudiar el rol de los mecanismos de disuasión en el ámbito cibernético desde la dimensión normativa propuesta por la metodología adoptada, la principal discusión condujo a responder la hipótesis planteada, la respuesta cibernética por parte de Rusia se dio considerando que las vulnerabilidades de Estonia en el plano cibernético frente a la falta de mecanismos de disuasión ofensivos generaban un esquema de altos beneficios y bajos costos para Rusia. El elemento disuasivo de la OTAN ponía en jaque la plausibilidad de un ataque militar ruso, mientras que la ausencia de reglas claras sobre el ciberespacio en términos de definir lo que se considera un ataque abrieron la posibilidad de un acto ofensivo de bajo costo y altos beneficios.

Palabras clave

Realismo estructural, teoría de juegos, ciberdisuasión, Estonia, Rusia.

Abstract

In 2007 Estonia suffered a series of disruptive cyber-attacks by Russia that positioned cyberspace as a new battlefield. From the academy, many sought to give several explanations on why Russia developed this attack. However, few analyses inquired about the decision to conduct a cyberattack over other possible options, such as resorting to conventional means just as diplomatic, economic or military ones. This paper aims to analyze the causes for which Russia chose such means and not another, explained from the hypothetical-deductive perspective of game theory. Likewise, it is proposed to study the role of deterrence mechanisms in the cyber field from the normative dimension proposed by the methodology adopted. The main discussion led to answer the hypothesis raised, the cyber response by Russia was given considering that Estonia's vulnerabilities in the cybernetic plane in the face of the lack of offensive deterrence mechanisms generated a scheme of high benefits and low costs for Russia. The dissuasive element of NATO put in check the plausibility of a Russian military attack, while the absence of clear rules on cyberspace in terms of defining what is considered an attack opened the possibility of an offensive act of low cost and high benefits

Keywords

Structural realism, game theory, cyber-deterrence, Estonia, Russia.

La Internet fue originalmente diseñada con el propósito de interconectar una acotada serie de redes. La idea de que esté a disponibilidad de todos resultaba un hecho poco probable. Sin embargo, el tiempo pasó, los protocolos se desarrollaron y las redes evolucionaron, expandiéndose a todos los lugares del mundo. Hoy, como consecuencia de una de las revoluciones tecnológicas más importantes de la historia, Internet ha permitido que el mundo se encuentre globalmente interconectado (Bodmer, 2017).

Con el desarrollo y la expansión constantes del ciberespacio, todos aquellos desafíos que representaban las distancias físicas y los largos períodos de tiempo para la comunicación se desvanecieron. No obstante, a la par, surgieron nuevas amenazas que plantearon preguntas sobre la evolución de las medidas de seguridad no sólo para el sector privado sino también para los Estados, quienes tienen la responsabilidad última de proteger las Infraestructuras Críticas[i] con sede en su territorio (Carlini, 2016: 67).

La importancia del ciberespacio como quinta dimensión a proteger tomó mayor relevancia a nivel internacional principalmente a partir de los acontecimientos del caso de Estonia en 2007 y el de Stuxnet en 2010 (Carlini, 2016: 66). Si bien la ciberseguridad puede ser analizada desde múltiples áreas como el hackactivismo, ciberterrorismo o ciberespionaje, sin dudas uno de los desafíos más significativos que se presenta en el ámbito cibernético en términos de seguridad para los Estados es el de la ciberguerra (Nye, 2015). Tal como lo explican Singer y Friedman en *"Cybersecurity and cyberwar: what everybody needs to know"* (2014: 120), la noción de "ciberguerra" encarna un problema para los Estados porque en principio abarca un espectro muy amplio de comportamientos: desde campañas de cibervandalismo y disrupción hasta un real estado de guerra utilizando medios cibernéticos. Sin embargo, los autores entienden que existe una lógica propia en la ciberguerra, al igual que en todas las guerras en otros espacios: siempre tiene un modo y objetivo político, por un lado, y por otro, siempre implica un determinado elemento de violencia.

Considerando esto, en la presente investigación se propone que no sólo las capacidades defensivas son importantes en el ciberespacio para evitar ataques (o disminuir su efecto), sino que las capacidades ofensivas que generan esquemas de disuasión toman un rol central como una posible estrategia de los Estados para evitar convertirse en objetivos de ataques por parte de terceros.

Ahora bien, en la quinta dimensión existen diferentes problemas para aplicar mecanismos de disuasión. Según Nye (2015) y Feaking (2015) existen dos dificultades principales en la quinta dimensión: por un lado, la cuestión de la identidad o el origen,

donde explican que es atribuirle identidad al atacante resulta una tarea muy ardua; y por el otro, la cuestión del tiempo y cómo este implica un factor determinante a la hora de establecer cuáles fueron los daños y cuál podría ser una respuesta plausible.

El ciberataque de Rusia a Estonia en la primavera del 2007 ofrece un ejemplo de la naturaleza de la ciberguerra y la incertidumbre y ambivalencia existentes dentro de la comunidad internacional sobre cómo responder a esta clase de ataques (Barletta, 2017: 481). Fue el primer ciberataque conocido contra la totalidad de un país, exponiendo las vulnerabilidades del país báltico a las disrupciones cibernéticas y a su vez poniendo en relieve las capacidades ofensivas de Rusia en el campo ciberespacial que dieron lugar a otros ataques posteriores como el de Georgia en 2008 y Ucrania. Previo al ataque, los ataques cibernéticos no habían sido considerados como una amenaza inminente para el Estado y/o sus ciudadanos. Este hecho marcó un punto de inflexión en la percepción del ciberespacio como un potencial dominio de operaciones y es relevante para interpretarlo como un antecedente que manifestó la necesidad de adoptar medidas y desarrollar una estrategia de ciberdefensa, principalmente en el marco de la Unión Europea y específicamente en el de la Organización del Tratado del Atlántico Norte (OTAN).

A finales de abril del 2007 las autoridades de Estonia decidieron quitar la Estatua de Bronce que evocaba la, para algunos, oscura etapa soviética del país del Báltico. Como reacción a tal disposición se dieron múltiples manifestaciones en la plaza principal en Talín y en simultáneo los principales entes políticos, financieros y comunicación del país comenzaron a sufrir ataques cibernéticos de tipo DDoS (*distributed denial-of-service*). El Ministro de Justicia estonio culpó a Rusia de perpetrar los ataques, y, en consecuencia, Moscú desestimó tales acusaciones y dio la directiva de desviar su negocio de cargas del puerto de Talín a los puertos de Letonia y Lituania como castigo.

Lo que aún resulta una incógnita es por qué Rusia decidió realizar un ciberataque. Si bien Ganuza Artiles (2011) plantea que algunas posibles razones podrían ser la percepción de Rusia de la dependencia de tecnologías como vulnerabilidad para el país báltico y el ciberataque como forma de poner a prueba las capacidades cibernéticas tanto de la Unión Europea como de la OTAN, estas no son más que hipótesis sin sustento empírico para comprobarlas.

A partir de esta situación, cabe preguntarse concretamente por qué Rusia optó por ejecutar un ciberataque frente a otras opciones a su disposición para cumplir sus objetivos. Para dar respuesta a esta pregunta, en el presente trabajo se elaboró un modelo hipotético-deductivo basado en la teoría de juegos a fin de dar cuenta de las

opciones disponibles para Rusia y el escenario que podría haber llevado a los líderes rusos a tomar tal decisión. Conforme a lo planteado, fue necesario describir las relaciones bilaterales en materia de economía, política y seguridad entre Estonia y Rusia; modelizar el caso del ciberataque de Rusia a Estonia a partir de la teoría de juegos; indagar las posibles respuestas de Estonia al ciberataque, considerando sus pertinentes costos y ganancias; y, por último, desarrollar el rol de los mecanismos de disuasión en el espacio cibernético.

Indagamos el rol de los mecanismos de disuasión como variable interviniente moderadora en la relación entre las motivaciones y la ejecución de un ciberataque. Las motivaciones son definidas como la serie de razones que provoca la realización u omisión de un ciberataque; los mecanismos de disuasión se entienden como el conjunto de formas de penalización que determinan la retaliación hacia el perpetrador del ciberataque; y la ejecución de un ciberataque hace referencia al tipo de ataque a ejecutar y a la probabilidad de su ejecución, considerando la variable moderadora de los mecanismos de disuasión.

Planteamos como hipótesis que los mecanismos de disuasión, planteados en términos de capacidades (cibernéticas o convencionales ofensivas), disminuyen la probabilidad de ataques cibernéticos de gran escala. En este sentido, un Estado puede tener motivaciones para realizar un ciberataque a otro, pero si el potencial actor agredido tiene mecanismos de disuasión eficaces, el agresor ejecutará un ciberataque menos dañino del esperado originalmente o se abstendrá de ejecutar cualquier tipo de acción en este sentido. Aplicado al caso de Estonia, planteamos que, más allá del rol de las capacidades defensivas, si el país báltico hubiese tenido mecanismos ciber-disuasivos efectivos, Rusia no hubiese ejecutado el ciberataque.

Una metodología que resulta útil para analizar la interacción estratégica de los actores en este caso en particular es la teoría de juegos, la cual se centra en el estudio del comportamiento estratégico a partir de la interacción de dos o más actores en un modelo llamado “juego” y la decisión individual que toman a partir de lo que esperan que los otros hagan (Monsalve, 2002). La teoría de juegos resulta valiosa en el ámbito de las Relaciones Internacionales en tanto hace énfasis en el proceso de toma de decisiones de los líderes. Siguiendo a Renshon y Renshon (2008: 511), “ninguna crisis o guerra puede ser entendible sin referencia directa a la toma de decisiones de los líderes individuales”[ii].

Tomando el caso de Estonia como ejemplo concreto de ciberguerra, esta investigación planteó su análisis a partir de las lógicas propias del realismo estructural de Waltz (2000) y, en un plano más específico, conforme a los postulados planteados en la teoría de la disuasión del ciberespacio desde la perspectiva de Will Goodman (2010). Cabe aclarar que adoptamos una perspectiva en línea con lo que Graham Allison (1971) plantea como el Modelo del Actor Racional, en tanto las decisiones políticas están vistas como acciones voluntarias y con propósitos claros basado en cálculos de utilidad y entendiendo que los actores tomadores de decisiones son los Estados o sus gobiernos nacionales, quienes actúan conforme a sus intereses y objetivos a alcanzar.

Conforme a los postulados teóricos y el modelo planteados en este trabajo, si Estonia hubiese tenido mecanismos ofensivos fuertes que hubiesen generado esquemas de disuasión en el espacio cibernético y considerando los altos costos de ejecutar otras opciones disponibles, las probabilidades de un ciberataque por parte de Rusia como respuesta no sólo habrían disminuido, sino que habrían limitado la posibilidad de responder con cualquier otro acto retaliatorio que implique daños significativos para Estonia.

En la primera sección del trabajo se desarrollan las bases teóricas que definen el marco de la investigación. En la segunda, se describen las relaciones bilaterales de Estonia y Rusia y se explican los intereses de Rusia en los países bálticos y por qué el ciberataque a Estonia estaba justificado desde la perspectiva rusa. En la tercera, se analiza el caso de Rusia y Estonia desde la teoría de juegos, modelizando un juego inicial donde no se toman en consideración las probabilidades de ocurrencia de los escenarios de victoria de ambos jugadores (Rusia y Estonia) en una instancia de enfrentamiento militar convencional y un segundo juego donde sí se consideran tales probabilidades. En la cuarta, se examinan los resultados de los nodos finales del último juego, interpretando en cada caso la lógica existente de los pagos para cada jugador. En la quinta, se expone un nuevo juego donde se explica qué podría haber pasado si Estonia hubiese tenido una estrategia de ciberdisuasión sólida. Por último, se plantean las conclusiones abordadas, se examinan los alcances de este trabajo, las limitaciones y las posibles futuras líneas de investigación.

1. Hacia la ciberdisuasión

Siguiendo la lógica del realismo estructural, la disuasión se presenta como una alternativa que tienen los Estados para aplicar antes de que comience un conflicto, con

el fin de evitarlo, pero también una vez que comenzaron a darse las hostilidades, buscando limitar el alcance de tales ataques y potencialmente poseer el dominio de la escalada (Jordán, 2014). En términos de Waltz, la disuasión en general implica "… persuadir a alguien de una determinada acción asustando a esa persona con las consecuencias que traería llevar a cabo tal acción" (1990: 732).

Según Will Goodman, la disuasión consta de ocho elementos: un interés, una declaración de disuasión, medidas de denegación, medidas de penalización, la credibilidad, la seguridad, el miedo y el cálculo costo-beneficio (2010: 7). La lógica entre estos elementos se define a partir de que un Estado emplea una estrategia de disuasión para proteger un determinado interés; para advertir a sus adversarios (quienes representan una amenaza para tal interés) el Estado hace una declaración de disuasión, donde se formula la idea de "No hagas esto, o tal/es cosa/s va/n a pasar" y para efectivizar tal proposición presenta medidas de denegación, medidas de penalización o ambas; y para que los Estados adversarios tomen en serio la declaración de disuasión esta debe ser creíble y asegurada.

A partir de tal esquema vale aclarar: la credibilidad implica que la disuasión sea posible y probable; la seguridad significa que si el adversario no pone en riesgo el interés del Estado disuasor, se asegure que no recibirá penalizaciones; el miedo juega un rol primordial en tanto un adversario con miedo será menos propenso a realizar una acción que ataque el interés del otro Estado; la denegación es un aspecto defensivo de la disuasión (consiste en la prevención y en la inutilidad) y la penalización se considera como un aspecto ofensivo (consiste en retaliación, interdependencia y contradependencia).

En síntesis, las reflexiones generales sobre la teoría de la disuasión pueden resumirse en:

- La disuasión consta de un elemento cuantitativo y uno cualitativo: por un lado, la existencia de los elementos necesarios para generar disuasión, y por el otro, la capacidad de tales elementos de asegurar un *second-strike* efectivo para alcanzar los objetivos previstos.
- A mayores capacidades, mayor poder de disuasión: si el Estado disuasor tiene altas capacidades de contraataque, el Estado adversario se verá menos motivado a realizar un ataque considerando que dentro del cálculo costo-beneficio, los costos de realizar el ataque podrían ser más altos que los beneficios.

- A mayor tiempo de respuesta, menor efecto disuasorio: mientras más largo sea el período de tiempo que se dé entre el ataque efectuado y la retaliación, menor será el efecto disuasorio porque la lógica de la disuasión implica un contraataque inmediato al ataque recibido.

- A menor credibilidad de retaliación, menor disuasión: la declaración de disuasión debe ser creíble para que el adversario interprete los riesgos a los que se somete en caso de ejecutar un potencial ataque.

- La retaliación debe seguir una lógica de proporcionalidad: un contraataque superior al ataque recibido puede generar un escalamiento del conflicto y/o implicar un costo reputacional alto apara el agente disuasor.

Goodman (2010) entiende que la ciber-disuasión, tal como cualquier otro tipo de disuasión (nuclear, convencional, etc.) tiene éxito cuando el adversario decide no actuar de forma agresiva. Los presupuestos de toma de decisiones en el ciberespacio implican considerar que el tomador de decisiones no siempre tiene la información completa y perfecta de un determinado escenario, llevando muchas veces a errores de cálculo. A partir de esta reflexión, el autor sintetiza su teoría de la ciber-disuasión en seis grandes puntos.

En primer lugar, los Estados deben comunicarse constantemente para asegurarse que los mensajes de seguridad estén proyectados, recibidos y entendidos: si los Estados constantemente intercambian mensajes de ciber-disuasión, pero lo hacen en silencio y con poca fanfarria, probablemente prevalecerán los ataques cibernéticos.

Segundo, los Estados deben mantener medidas de denegación efectivas y medidas de penalización creíbles y amenazantes: las medidas de denegación disminuyen los beneficios de realizar un ciberataque, pero lo que realmente define la ejecución son las medidas de penalización (si un adversario se enfrenta a medidas de denegación, pero no tiene penalizaciones, continuará realizando los ataques hasta que pueda encontrar y aprovechar una determinada vulnerabilidad).

En tercer lugar, si son atacados, los Estados-víctima deben tener la capacidad de identificar el o los responsables del ciberataque con seguridad, ya sea mediante una investigación efectiva o a partir de la responsabilidad asignada: el Estado que disuade primero debe saber quién fue el atacante para realizar un contraataque, y para ello pueden asumir una investigación para descubrir el origen del ataque (lo cual requiere

muchos recursos y tiempo) o pueden establecer acuerdos de asistencia legal mutua para asignar la responsabilidad de ataque al Estado que no coopera.

En cuarto, los Estados deben asegurarse de que al menos algunas de sus capacidades de contraataque no puedan ser deshabilitadas en un ciberataque de *first-strike*: es difícil de determinar porque la naturaleza de los *malwares*, por ejemplo, es expandirse, pero no dar índices de cuándo o hacia dónde lo harán.

Quinto, el Estado que disuade debe tener simetría geopolítica (y sino, una asimetría favorable) donde tenga la capacidad efectiva de disuadir a sus adversarios: si la asimetría es desfavorable, no podrá protegerse a sí mismo a medida que el conflicto en el ciberespacio se intensifique y pueda tener repercusiones graves en el mundo físico.

Finalmente, la ausencia de promesas de seguridad puede obstaculizar que los Estados establezcan una relación de disuasión cibernética: asegurar medidas de denegación y penalización dará un panorama de tranquilidad donde las promesas de dar ciertos tipos de ciberataques implicarán una "invitación a que los adversarios sean víctimas" (et. al.: 109).

Estas premisas serán analizadas a partir del caso del ciberataque de Rusia a Estonia en el año 2007 desde un modelo hipotético deductivos desde la teoría de juegos a fin de analizar las posibles consecuencias de un esquema de disuasión formado por capacidades ofensivas por parte de Estonia. En línea con la teoría presentada, nuestro modelo indica que, frente al alto costo de otras opciones disponibles, el aumento de las capacidades ofensivas de Estonia no solamente habría disminuido las probabilidades de un Ciberataque, sino que hubiera prácticamente eliminado las posibilidades de cualquier acto represivo por parte de Rusia. A fin de realizar este análisis, primero debemos abocarnos a la descripción de las relaciones bilaterales entre ambos actores previas al evento analizado en cuestión.

2. Las relaciones bilaterales entre Rusia y Estonia

Las relaciones entre Estonia y Rusia pueden encontrar su origen en el siglo XVIII cuando el Imperio Ruso anexó a Estonia luego de la derrota a Suecia en la Gran Guerra del Norte. Estonia fue identificada como una provincia báltica hasta 1918 donde se declara la Guerra de Independencia, habiendo transcurrido ya la Primera Guerra Mundial y la Revolución Rusa de 1917. Con el Tratado de Tartu se firmó la paz entre ambos países, donde la Rusia soviética reconoció la soberanía de Estonia y renunció a todos los reclamos territoriales sobre ese país.

Durante años posteriores, las relaciones políticas entre ambas naciones se desarrollaron entorno a lo que fue el Segundo Congreso Internacional Comunista en Rusia En el ámbito económico, la independencia de Estonia significó una gran fuga de capitales y la retirada de los mercados tradicionales de Rusia. De tal forma, el país báltico buscó estructurar un nuevo sistema monetario y se propuso la creación de un puente que conectase la Rusia soviética con el oeste europeo.

Ya en el contexto de la Segunda Guerra Mundial, las relaciones entre Estonia y la Unión de Repúblicas Socialistas Soviéticas (URSS) se complejizaron. Cuando la URSS invadió Polonia, Estonia fue cuestionada por Rusia y Alemania frente a su neutralidad en dejar escapar un submarino polaco que se encontraba ubicado en el puerto de la capital estonia de Talín. A partir de este hecho, el gobierno en Moscú le exigió a Estonia que permitiese el establecimiento de bases militares soviéticas en territorio estonio. En principio el pacto fue aceptado y a cambio la URSS se comprometió a aumentar las transacciones comerciales con Estonia. Además, se acordó entre ambos países un pacto de defensa mutua frente a cualquier agresión proveniente de alguna potencia europea.

Entrando en la década de 1940, la Unión Soviética desplegó un bloqueo militar de Estonia, desencadenando poco tiempo después un golpe de Estado en el país báltico apoyado por las tropas soviéticas que se encontraban en territorio estonio. En ese mismo año el Parlamento proclamó a Estonia como una República Socialista y solicitó que fuera aceptada en la Unión Soviética. La ocupación soviética se dio de forma efectiva desde 1944 hasta 1991. En términos políticos, Estonia fue administrada desde Moscú a través de gobernadores estonios nacidos en Rusia. En términos económicos, la Estonia soviética fue parte de una serie de reformas económicas experimentales durante la década de 1950 que luego se replicarían en el resto de los países pertenecientes a la Unión Soviética.

La decadencia del gobierno en Moscú implicó un deterioro en las relaciones de poder con las naciones anexadas a la Unión Soviética, y para 1990 se eligió libremente un nuevo Parlamento en Estonia donde se aprobó la resolución de independencia de la Estonia soviética que pasaría a llamarse República de Estonia. En 1991 el Consejo de Estado de la Unión Soviética reconoció la independencia de Estonia y recién en 1994 las últimas tropas rusas se retiraron del territorio estonio. Con la independencia de Estonia se firmó un tratado entre el país báltico y Rusia donde se acordaba la garantía del gobierno estonio de darle el derecho a los antiguos residentes de la Estonia soviética de elegir libremente su ciudadanía. Para fines de la década de 1980, más del 60% de los

ciudadanos eran de etnia estonia y la segunda gran etnia era rusa con el 30% (Park, 1994: 71). Pese a ello, el gobierno estonio buscó aplicar políticas de ciudadanía que produjesen grandes cambios en la composición étnica para asegurarse que no volviese a ocurrir un nuevo episodio de ocupación rusa. Sin embargo, para 1993 se simplificaron las reglas para aplicar a la ciudadanía.

Aunque la cuestión étnica permaneció latente, el gobierno estonio continuó enfocándose en la cooperación transfronteriza con Rusia en términos de infraestructura, transporte, aplicación de la ley, educación, cultura y salud. Para 2007 la coalición gobernante acordó una serie de políticas que llamasen a iniciativas de desarrollo de relaciones cooperativas entre Estonia y Rusia. Esta nueva etapa en las relaciones bilaterales entre Estonia y Rusia buscaron dejar atrás el pasado soviético y la rivalidad con Rusia y a su vez fue complementada con el ingreso de Estonia a la Unión Europea y occidental con el ingreso a la OTAN.

Parte del espíritu de la nueva política exterior de Estonia post-era soviética se proyectó en el deseo de las autoridades estonias de mover una estatua conmemoratoria de un soldado ruso de la Segunda Guerra Mundial de la plaza principal en Talín hacia el cementerio militar de la capital estonia. El Soldado de Bronce fue considerado un símbolo de los caídos durante la guerra por la comunidad rusa en Estonia, pero por otro lado para los ciudadanos de etnia estonia fue percibido como un símbolo de la era soviética a la cual no desean retornar (Ganuza Artiles, 2011: 174). Con el anuncio de la retirada de la estatua y la ya existente polarización en crecimiento, se produjeron manifestaciones similares que acabaron con más de 1.000 arrestados, varios heridos y un muerto.

Con la agudización del conflicto, se sumó otro hecho: comenzaron a darse simultáneos ataques cibernéticos de tipo DDoS (*distributed denial-of-service*) a los principales entes políticos, financieros y de comunicación de este país, hecho que generó una parálisis a nivel estatal durante casi un mes.

La reacción automática del gobierno estonio fue culpar a Rusia: el Ministro de Justicia de Estonia Rein Lang afirmó que los ataques habían podido ser rastreados a direcciones IP en Moscú de propiedad del gobierno de Rusia, acusación que siempre fue desestimada por los principales dirigentes de este país. Frente a esto, Rusia comenzó a desviar su negocio de cargas del puerto de Talín a los puertos de Letonia y Lituania como castigo frente a tales acusaciones (Schmidt, 2013: 17).

En el 2009, empero, Konstantin Goloskokov, un activista del grupo juvenil Nashi de Rusia y asistente de un miembro parlamentario pro-Kremlin, se responsabilizó por el ciberataque del 2007. Justificó su accionar entendiendo que fue un modo de protesta contra el desmantelamiento del monumento del Soldado de Bronce. Desde su perspectiva, el ciberataque no fue ilegal, sino más bien fue un acto de desobediencia civil (Lowe, 2009).

La gran repercusión del ataque se fundamenta en que Estonia es considerada como uno de los países pioneros en promover iniciativas para la digitalización del Estado, poseyendo los niveles más altos del Índice de Desarrollo del Gobierno Electrónico de la ONU (Heath, 2019). Es por ello por lo que el alto grado de dependencia que tiene Estonia con Internet, la convierte en más vulnerable a sufrir disrupciones cibernéticas.

Ahora bien, considerando el desarrollo de las relaciones bilaterales entre Rusia y Estonia, resulta innegable aceptar que, desde la llegada de Putin al poder, Rusia se ha configurado como una amenaza para el país de la región del Báltico. En los documentos de seguridad nacional de Estonia se toma a Rusia como una amenaza a la seguridad nacional, teniendo en consideración la presencia militar de Rusia en las fronteras de Estonia (Estonia Ministry of Defence, 2011).

Con el fin de la Guerra Fría y la disolución de la Unión Soviética, los países del Báltico retomaron su independencia y pocos años después comenzaron a integrarse al bloque occidental mediante el ingreso a la Unión Europea y a la OTAN. De esta forma, Rusia y la Alianza de Seguridad comenzaron a compartir una frontera de más de 500 mil kilómetros (Lee Myers, 2004). Aún más, Vladimir Putin interpreta que la relación entre Rusia y la OTAN se da como un juego de suma cero: cada avance de la Alianza implica una pérdida para Rusia ya sea en términos de poder o influencia (Kyle, 2018). En este sentido, es el miedo al avance de la OTAN el justificativo para tomar acciones de política exterior agresivas que ponen en riesgo la seguridad del Estado ruso.

La plausible intervención de Rusia en asuntos internos tanto de Estonia como del resto de los países de la región se fundamenta en primera instancia, porque en su momento estos países fueron miembros de la Unión Soviética, y en segunda, porque ellos poseen una población significativa de ciudadanos ruso étnicos por los cuales deben velar el cumplimiento de sus derechos (Kyle, 2018: 108).

De forma evidente, el temor reaccionario de los países bálticos viene acompañado de la idea de volver al fantasma soviético. Si bien resulta poco probable una invasión rusa, particularmente considerando que Estonia, Lituania y Letonia pertenecen a la OTAN,

Rusia dispone de tácticas asimétricas que le permiten mantener a tales países bajo su órbita de influencia, y en estos términos uno de los casos que dan muestra de ello es el de Estonia en el 2007.

Sin embargo, si bien se esperaba una reacción por parte de Rusia frente a la directiva de mover la estatua, la incógnita que surge es por qué se recurrió a un ciberataque y no a otro tipo de respuesta. Considerando esto, en los siguientes apartados se pretenderá abordar una explicación de estos eventos desde la racionalización del cálculo estratégico que permite la teoría de juegos.

Resultados

Interacción estratégica entre Rusia y Estonia: el juego

Habiendo indagado sobre las relaciones bilaterales entre ambos países, cabe analizar por qué, frente a las acciones llevadas adelante por Estonia, Rusia decidió ejecutar un ataque disruptivo sobre las Infraestructuras Críticas y no optó por otro tipo de medidas, como sanciones económicas o acciones militares convencionales. En este sentido, la teoría de juegos resulta útil para analizar el comportamiento estratégico de ambos actores y explicar las acciones resultantes de su interacción.

Basada en la teoría de la utilidad, la teoría de juegos asume que los actores enfrentan diferentes conjuntos de acciones disponibles y deben tomar una decisión siguiendo la lógica de utilidad, entendida como una medida de las preferencias del actor sobre los resultados que reflejan su voluntad de asumir riesgos y evitar resultados indeseables para lograr los resultados deseados. Así se destacan dos dimensiones: una normativa, que pretende explicar cuál sería el comportamiento estratégico óptimo de los jugadores involucrados en un juego; y una descriptiva, que busca explicar los movimientos que los jugadores efectivamente llevaron a cabo en una situación concreta según su racionalidad (Morrow, 1994).

El juego que se modela a continuación pretende explicar el caso del ciberataque de Rusia a Estonia en el año 2007. El mismo fue modelado como un juego no cooperativo, donde los agentes o jugadores toman sus decisiones en forma independiente sin tener ningún compromiso con los demás participantes del juego. En este sentido cabe interpretar que los intereses de Rusia son contrapuestos a los de Estonia. Además, el juego está esquematizado de forma extensiva, donde a partir del esbozo de un árbol de decisiones se da cuenta de las opciones tomadas, en tanto consideramos que estas no

tuvieron un carácter simultáneo, sino más bien secuencial (Pérez, Jimeno y Cerdá, 2004).

Por otro lado, este juego se compone en principio como uno de información perfecta donde el conjunto de información de cualquiera de los jugadores es unitario (Ibidem, 2004). No obstante, presenta tres posibles acciones o decisiones que conllevan a "sub-juegos" caracterizados por la información imperfecta de sus nodos finales, en tanto presentan situaciones de guerra o conflicto armado (caracterizadas por el carácter probabilístico y no determinado de su desenlace)[iii].

El juego está basado en una lógica de suma cero, donde a mayores ganancias para uno de los jugadores, mayores pérdidas para el otro. En este aspecto, las acciones o decisiones disponibles fueron elegidas tomando como supuesto que los principales métodos de gestión de conflictos internacionales son los medios tradicionales de influencia diplomática, militar y económica, que pueden incluir la amenaza o el uso de la fuerza (Committee on International Conflict Resolution, 2000). A esta batería de opciones se le agrega la respuesta cibernética, que expone la existencia de nuevas herramientas a disposición de los Estados que son plausibles de ser utilizadas en el marco de la búsqueda de sus respectivos intereses nacionales.

Considerando las partes desarrolladas anteriormente, el juego representado a continuación debe ser interpretado de la siguiente manera:

- **Jugadores:** el juego se compone de dos jugadores quienes serán denominados Jugador 1 o J_1, correspondiente a Rusia, y Jugador 2 o J_2, referente a Estonia.
- **Acciones:** tanto para el J_1 como para el J_2 las acciones posibles se limitan a No Responder (NR), Responder por vía Económica y/o Diplomática (RED), Responder por vía Militar (RM) o Responder por vía Cibernética (RC).
- **Pagos:** debido a que la información disponible no permite definir el grado de preferencia de pagos de ambos jugadores en términos de intervalos, la estructura de los pagos debe ser interpretada como una escala ordinal de preferencias, entendiendo que 1 (uno) es el escenario menos deseado y 18 (dieciocho) el más favorable a cada jugador. En el Gráfico 1 los pagos se encuentran distribuidos en cada nodo terminal, definiendo primero los pagos para el J_1 y seguido los pagos para el J_2.

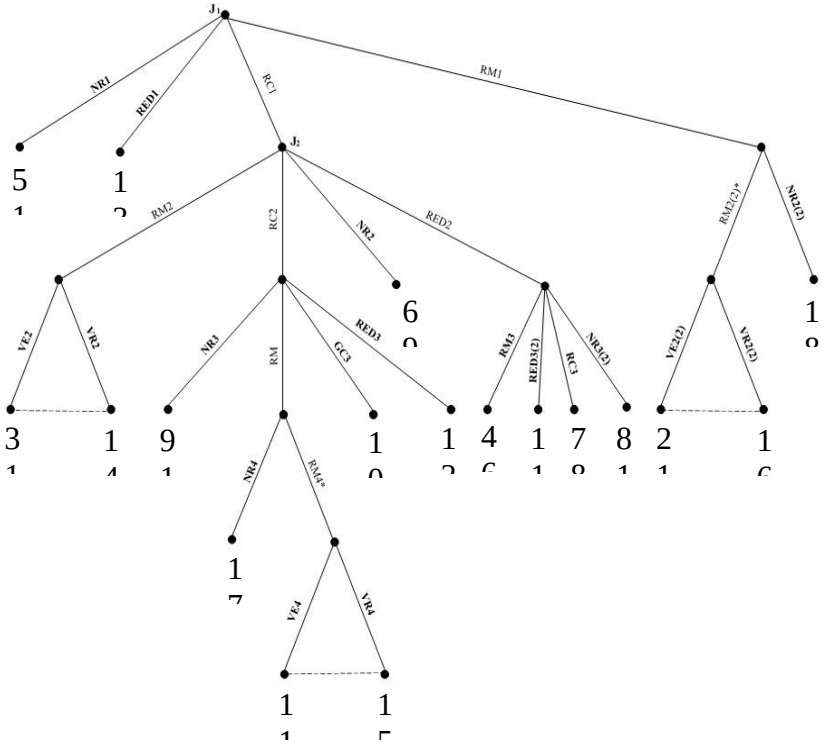

Gráfico 1. Representación gráfica en forma extensiva del juego modelado Interacción estratégica entre Rusia y Estonia 2007

En la siguiente tabla se especifican los acrónimos existentes en el juego. El número que le sigue a cada acrónimo corresponde al sub-juego en el que se encuentra, siendo 1 el primer sub-juego y 4 el último.

Tabla 1
Acrónimos del juego

NR	No Responde
RED	Responde por vía Económica y/o Diplomática
RM	Responde por vía Militar
RM*	Responde por vía Militar con respaldo de la OTAN
RC	Responde por vía Cibernética
GC	Guerra Cibernética
VE	Victoria de Estonia
VR	Victoria de Rusia

Tal como puede observarse, el juego parte desde el supuesto de que Estonia, de ahora en más J_2, quita la estatua del Soldado de Bronce de la plaza de Talín y Rusia, a partir de ahora J_1, tiene la posibilidad de escoger entre No Responder (NR), Responder por la vía Económica y/o Diplomática (RED), Responder por vía Cibernética (RC) o Responder por vía Militar (RM). Siguiendo el juego, se analizan las posibles respuestas del J_2 en caso de que el J_1 opte por la acción de RM o la de RC: en la primera podrá optar por NR o RM, teniendo el respaldo de la OTAN; mientras que en la segunda podrá escoger entre la acción NR, RM sin tener el respaldo de la OTAN, RED y RC. En el tercer sub-juego, el J_1 puede responder a la acción de RC o a la de RED del J_2: tanto en el primero como el segundo caso podrá elegir entre NR, RM, RC (denominado GC en el primer caso) y RED. Por último, en el cuarto sub-juego, el J_2 podrá responder sólo en caso de que el J_1 haya escogido RM, teniendo la posibilidad de NR o RM.

La Tabla 2 muestra el orden de pagos para cada jugador, entendiendo que 1 (uno) representa el peor escenario y 18 (dieciocho) el mejor. De forma similar, la Tabla 3 presenta los pagos para cada jugador tomando los nodos terminales del juego y comparando los pagos según el escenario descrito. En esta primera instancia se analizan los pagos sin tomar en consideración la plausibilidad de una victoria de Estonia o de Rusia en caso de un conflicto militar en términos probabilísticos.

Tabla 2 –
Estructuración de pagos para el J_1 (Rusia) y J_2 (Estonia) del peor escenario al mejor escenario

	J_1 – Rusia	**J_2 – Estonia**
1	VE4	NR2(2)
2	VE2(2)	NR4
3	VE2	VR2(2)
4	RM3	VR2
5	NR1	VR4
6	NR2	RM3
7	RC3	GC3
8	NR3(2)	RC3

Tabla 3 –
Estructuración de pagos para el J_1 (Rusia) y J_2 (Estonia) según comparación de pagos en cada escenario

	J_1 – Rusia	**J_2 – Estonia**
NR1	5	13
RED1	13	12
VE2	3	18
VR2	14	4
NR2	9	15
VE2(2)	2	17
VR2(2)	16	3
NR2(2)	18	1

9	NR3	NR2	NR3	9	15
10	GC3	RED3(2)	GC3	10	7
11	RED3(2)	RED3	RED3	12	11
12	RED3	RED1	RM3	4	6
13	RED1	NR1	RED3(2)	11	10
14	VR2	NR3(2)	RC3	7	8
15	VR4	NR3	NR3(2)	8	14
16	VR2(2)	VE4	NR4	17	2
17	NR4	VE2(2)	VE4	1	16
18	NR2(2)	VE2	VR4	15	5

Nota. Denota el orden de pagos para cada jugador siendo uno el peor escenario y 18 el mejor.

Nota. Denota el orden de pago para cada jugador comparando el pago según el escenario

El juego inicial planteado en el Gráfico 1 muestra la estructuración de pagos sin tener en consideración las probabilidades de victoria de los jugadores en una instancia de enfrentamiento militar convencional. Sin embargo, es necesario hacer la distinción de dos posibles instancias de confrontación completamente diferentes para los jugadores moderadas por el factor del respaldo de la OTAN hacia Estonia. Una situación de enfrentamiento militar bilateral entre Estonia y Rusia pone en evidencia las asimetrías de capacidades a favor de Rusia. No obstante, si Estonia fuese respaldada por la OTAN, tales asimetrías se revierten de forma clara.

En este sentido, comparando las capacidades materiales de Rusia con las de Estonia, aquellas de Rusia son mayores: Rusia tenía un PBI de 1,67 billones de dólares contra el de Estonia de 14 mil millones; el presupuesto de defensa ruso era de 531 mil millones de dólares contra el estonio de 205 millones; y en términos de capacidades militares el personal activo de Rusia era de 1.027.000 soldados (entre ellos 395.000 en Armada, 142.000 en Marina y 160.000 en Fuerza Aérea) y tenía aproximadamente 20 millones de soldados en reserva, mientras que Estonia tenía 4.100 soldados activos (3.600 en Armada, 300 en Marina y 200 en Fuerza Aérea) y aproximadamente 16.000 soldados en reserva (International Institute for Strategic Studies, 2007).

Sin embargo, en un posible escenario de guerra entre la OTAN y Rusia, las capacidades de la Alianza eran altamente superiores: al momento del conflicto, la

OTAN reunía un presupuesto de defensa de más de 832 billones de dólares y aglutinaba más de 3,6 millones de soldados en Fuerzas Armadas (OTAN, 2011).

Considerando esto y analizando la información disponible[iv], puede estimarse que en un hipotético enfrentamiento militar convencional entre Rusia y Estonia las probabilidades de victoria rusa serían de 0.95/1, mientras que las de Estonia serían 0.05/1. Por otro lado, tomando un escenario donde Estonia sea respaldada por la OTAN, un enfrentamiento de este mismo tipo entre la Alianza de Seguridad y Rusia llevaría a la victoria de la OTAN con 0.8/1 probabilidades contra las de Rusia (0.2/1). La OTAN mantiene un nivel de disuasión general más alto que Rusia porque ni sus Fuerzas Armadas son lo suficientemente grandes ni su economía está sobradamente desarrollada como para hacer frente a una guerra prolongada contra la Alianza (Kyle, 2018).

En el juego existen tres acciones de guerra: RM2, RM2(2) y RM4. De esta forma, aplicando las probabilidades (siendo P probabilidades de Victoria de Estonia y 1-P probabilidades de Victoria de Rusia) para cada escenario, la reestructuración de los pagos para el J_1 (Rusia) es la siguiente:

$$RM2 = VE*P + VR*1-P$$
$$RM2 = 3*0.05 + 14*0.95$$
$$RM2 = 13,45$$

$$RM2(2) = VE*P + VR*1-P$$
$$RM2(2) = 2*0.8 + 16*0.2$$
$$RM2(2) = 4,8$$

$$RM4= VE*P + VR*1-P$$
$$RM4 = 1*0.8 + 15*0.2$$
$$RM4 = 3,8$$

Para el J_2 (Estonia), la reestructuración de los pagos en las instancias de guerra se define de la siguiente manera:

$$RM2 = VE*P + VR*1-P$$
$$RM2 = 18*0.05 + 4*0.95$$
$$RM2 = 4,7$$
$$RM2(2) = VE*P + VR*1-P$$

$$RM2(2) = 17*0.8 + 3*0.2$$

$$RM2(2) = 14,2$$

$$RM4= VE*P + VR*1-P$$

$$RM4 = 16*0.8 + 5*0.2$$

$$RM4 = 13,8$$

Sobre esta base, los nodos terminales de las acciones VE2, VR2, VE2(2), VR2(2), VE4 y VR4 se descartan y son reemplazados por los nuevos nodos terminales RM2, RM2(2) y RM4. En la Tabla 4 se ubican los pagos en una escala ordinal donde 1 (uno) es el peor escenario o el escenario menos deseado y 15 (quince) es el escenario más favorable o deseado. La Tabla 5 muestra la comparación de pagos de cada jugador considerando cada nodo terminal.

Tabla 4
Estructuración de pagos para el J_1 (Rusia) y J_2 (Estonia) del peor escenario al mejor escenario

	J_1 – Rusia	**J_2 – Estonia**
1	RM4	NR2(2)
2	RM3	NR4
3	RM2(2)	RM2
4	NR1	RM3
5	NR2	GC3
6	RC3	RC3
7	NR3(2)	NR2
8	NR3	RED3(2)
9	GC3	RED3
10	RED3(2)	RED1
11	RED3	NR1
12	RED1	RM4
13	RM2	NR3(2)
14	NR4	RM2(2)

Tabla 5
Estructuración de pagos para el J_1 (Rusia) y J_2 (Estonia) según comparación de pagos en cada escenario

	J_1 – Rusia	**J_2 – Estonia**
NR1	4	11
RED1	12	10
RM2	13	3
NR2	5	7
RM2(2)	3	14
NR2(2)	15	1
NR3	8	15
GC3	9	5
RED3	11	9
RM3	2	4
RED3(2)	10	8
RC3	6	6
NR3(2)	7	13
NR4	14	2

15	NR2(2)	NR3	RM4	1	12

Nota. Denota el orden de pagos en una escala Ordinal, siendo uno el peor escenario y 15 el mejor

Nota. Denota la comparación de pagos de acuerdo al orden nominal

Finalmente, habiendo reestructurado los pagos para ambos jugadores, el Gráfico 2 muestra el juego modelado. Las líneas resaltadas muestran el resultado del juego basado en los acontecimientos ocurridos en el caso. En la próxima sección se procede a comentar los nodos terminales y los pagos correspondientes para cada uno de los jugadores.

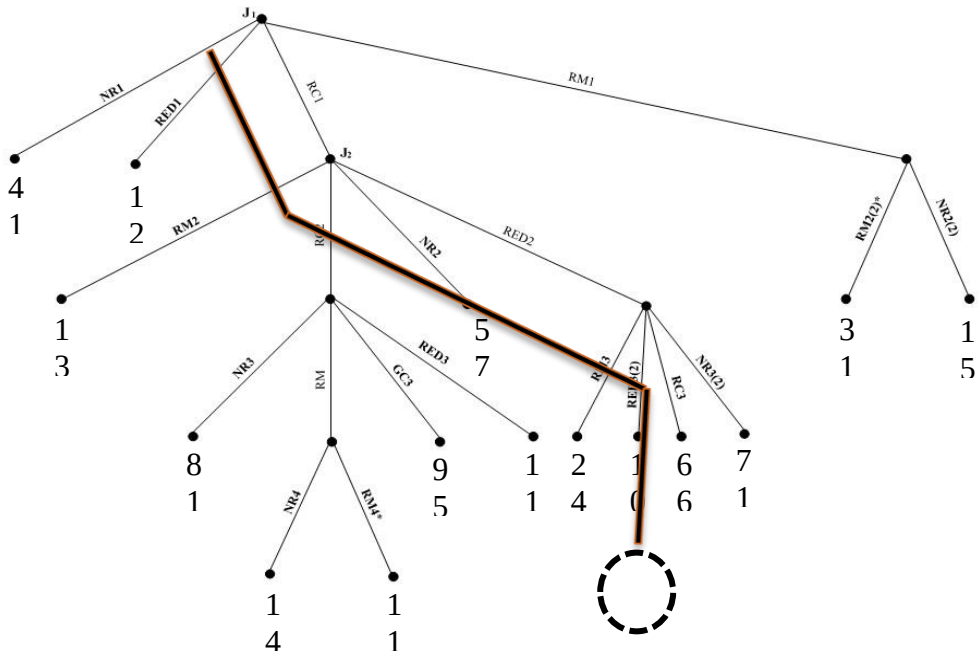

Gráfico 2. Representación gráfica en forma extensiva del juego modelado con la reestructuración de pagos

Interpretación de resultados

Habiendo considerado el orden de preferencias de los jugadores, es pertinente analizar los pagos de los nodos terminales que definen el comportamiento estratégico de los J_1 y J_2. Para ello se procederá a interpretar cómo se llegaron a esos nodos finales y qué implicancias tienen en las estructuras de los pagos de cada jugador.

SUBJUEGO 1: NR1 implica un mayor beneficio para Estonia (11) y una mayor pérdida para Rusia (4) porque Estonia no tiene consecuencias por haber movido la estatua y Rusia no es fiel a su doctrina geopolítica, mientras que **RED1** tiene un mayor beneficio para Rusia (12) y mayor pérdida para Estonia (10) porque se considera que la economía pequeña de Estonia es dependiente de las exportaciones de crudo y gas de Rusia (Grigas, 2012), por ende, una sanción económica podría generar distorsiones en la economía del país báltico.

SUBJUEGO 2: NR2 tiene mayores pagos para Estonia (7) que para Rusia (5) porque si bien un ciberataque genera costos para un país digitalizado como el de Estonia, no responder lo resguarda de un posible escalamiento del conflicto; **RM2** implica un mayor beneficio para Rusia (13) que para Estonia (3) porque el país báltico en tal caso no sería respaldado por la OTAN para la aplicación del Artículo 5 de su Tratado Constitutivo ya que Rusia no fue el país agresor[v]; **RM2(2)** expresa mayores pagos para Estonia (14) que para Rusia (3) porque la participación de la OTAN llevaría a que Rusia tenga pocas probabilidades de salir victorioso de una guerra convencional contra la Alianza; y **NR2(2)** tiene mayores costos para Estonia (1) que para Rusia (15) porque en caso de que Estonia no responda se asegura una victoria fácil.

SUBJUEGO 3: NR3 tiene mayores pagos para Estonia (15) en comparación con Rusia (8) considerando que Estonia lograría responder al ataque cibernético inicial y al no tener respuesta rusa evitaría una escalada del conflicto; **GC3** implica mayores costos para Estonia (5) que para Rusia (9) porque la alta dependencia de Estonia en el marco del ciberespacio la vuelve más vulnerable a sufrir disrupciones cibernéticas; **RED3** es más deseable por Rusia (11) que por Estonia (9) porque sigue la misma lógica que el escenario RED1; **RM3** tiene mayores pagos para Estonia (4) que para Rusia (2) porque sigue la misma lógica que RM2(2); en **RC3** tanto para Rusia como para Estonia los pagos son iguales (6) entendiendo que por un lado Estonia es vulnerable a sufrir nuevas disrupciones cibernéticas y por otro Rusia puede ser vinculada como perpetradora del ciberataque inicial en RC1; **NR3(2)** incluye mayores pagos para Estonia (13) por sobre los de Rusia (7) considerando que mediante la vía diplomática su reclamo puede ser escuchado en el marco de la Unión Europea o incluso de la OTAN, sumado a que la no respuesta de Rusia evita el escalamiento del conflicto; y por último, en **RED3(2)** con mayores pagos para Rusia (10) en detrimento con los de Estonia (8) se vuelve a definir la dependencia de la economía de Estonia con Rusia. Este escenario es el que se dio en

2007 cuando Rusia decidió responder ante la directiva del gobierno estonio de sacar la estatua, desviando su negocio de cargas del puerto de Talín a los puertos de Letonia y Lituania como castigo frente a las acusaciones de las autoridades estonias (Schmidt, 2013: 17).

SUBJUEGO 4: NR4 tiene mayores pagos para Rusia (14) que para Estonia (2) porque ante una respuesta militar rusa sin respuesta de Estonia, Rusia se asegura una victoria fácil; y **RM4** implica una mayor pérdida para Rusia (1) que para Estonia (12) porque en el caso de un enfrentamiento militar convencional Estonia cuenta con el apoyo de la OTAN y Rusia tiene muy pocas probabilidades de salir victoriosa.

El análisis de los nodos terminales muestra que, tomando lo ocurrido, el escenario RED3(2) era una circunstancia factible considerando los pagos para ambos jugadores. Ya sea para Estonia o para Rusia, los riesgos implícitos de adoptar una campaña militar u optar por no responder suponían ser muy altos. Para entender por qué efectivamente el escenario RED3(2) fue el que ocurrió resulta clave interpretar el hecho de que Estonia hubiese preferido optar por la vía diplomática, haciendo pública una declaración política sobre la culpabilidad de Rusia. Una respuesta económica de Rusia traería consecuencias para Estonia al corto plazo (tomando en cuenta su alta dependencia con la nación rusa en ese ámbito), sin embargo, efectuar tal declaración daría visibilidad a la problemática de las vulnerabilidades cibernéticas del país báltico, cuestión que podría ser abordada desde el marco de la OTAN e implicaría ganancias a futuro para Estonia, aún mayores que las de no recibir una respuesta económica por parte de Rusia.

El establecimiento de una estrategia colectiva de ciberseguridad orientada a la ciber-disuasión, interpretando la imperiosa necesidad de salvaguardar la seguridad de las Infraestructuras Críticas de los países miembros de la Alianza, generaría en estos términos el efecto disuasorio suficiente para anular la posibilidad de recibir otro ciberataque por parte de Rusia porque implicaría que, al definir a Rusia como una amenaza explícita dentro del ámbito ciberespacial, la Alianza tomaría medidas de penalización para neutralizar dicha amenaza.

Escenario normativo: la importancia de los mecanismos de disuasión

La teoría de juegos presupone el análisis de dos tipos de escenarios: uno descriptivo, donde se evalúa el comportamiento estratégico de los jugadores, y uno normativo, donde se reflexiona acerca del comportamiento óptimo para cada jugador (Morrow,

1994). Hasta ahora, en las secciones anteriores se abordó la dimensión descriptiva, mostrando la estructura de pagos para cada jugador basada en la información disponible del caso. En este sentido, para Estonia el recibir un ciberataque generaba altos costos por su alta dependencia a las redes cibernéticas, mientras que para Rusia implicaba una opción viable a llevar a cabo ya sea porque podía exponer las vulnerabilidades tanto de Estonia como de la Unión Europea y de la OTAN en su conjunto, además de que esta acción implicaba una demostración de capacidades ofensivas a partir de la ejecución de disrupciones cibernéticas[vi].

Sin embargo, si se toma la perspectiva normativa, la teoría de juegos permite analizar de forma hipotético-deductiva cuáles hubiesen sido los rendimientos óptimos para Estonia en el caso de haber tenido mecanismos de disuasión cibernética efectivos, incrementando los costos para Rusia en caso de elegir como respuesta la vía cibernética. Pero ¿qué determina una buena estrategia de ciberdisuasión? Will Goodman en *"Cyber Deterrence: Tougher in Theory than in Practice?"* hace un paralelismo entre la disuasión convencional y la cibernética interpretando que la disuasión per se consta de ocho elementos: un interés, una declaración de disuasión, medidas de denegación, medidas de penalización, credibilidad de la disuasión, seguridad de disuasión efectiva, miedo y cálculo costo-beneficio (2010: 7).

La dinámica existente entre estos elementos lleva a los fundamentos de la ciberdisuasión, entre los destacados: debe existir una constante comunicación donde se interpreten los mensajes de seguridad de forma correcta (y que, en caso de dar una declaración de disuasión, esta sea comprendida); deben darse medidas de denegación y penalización creíbles; en caso de ser atacado, un Estado debe tener la capacidad para identificar al perpetrador; el Estado disuasor debe tener una simetría geopolítica (o una asimetría favorable) con sus adversarios; y la ausencia de promesas de seguridad pueden obstaculizar la efectividad de una estrategia de ciberdisuasión.

Analizando el caso de Estonia una cuestión clave que define una estrategia de ciberdisuasión efectiva es la participación de la OTAN como instancia de intercambio de información para identificar cuándo se habla de un ciberataque y cuándo se trata de un ataque y no una mera intromisión sin intenciones de causar daño. En este sentido, las reglas de juego claras facilitan el abordaje del ciberespacio como dimensión a securitizar. Sin embargo, más allá de la OTAN, la necesidad de crear un acuerdo global

vinculante sobre las reglas de juego en el ciberespacio resulta imperativo para moderar el desarrollo de las capacidades cibernéticas de los Estados.

Sumado a esto, Estonia tiene una asimetría desfavorable con Rusia y en este contexto el respaldo de la OTAN puede convertirse en un factor que modifique esa relación de asimetría, donde ante una declaración de disuasión, Rusia capte el mensaje de que si efectúa un ciberataque recibirá una represalia.

Tabla 6
Estructuración de pagos para el J_1 (Rusia) y J_2 (Estonia) del peor escenario al mejor escenario en términos de escenario normativo

	J_1 – Rusia	**J_2 – Estonia**
1	RM4	NR2(2)
2	RM3	NR4
3	RM2(2)	RM2
4	NR1	RM3
5	NR2	NR2
6	RC3	RED3(2)
7	GC3	RED3
8	NR3(2)	RED1
9	NR3	RC3
10	RED3(2)	GC3
11	RED3	NR1
12	RED1	RM4
13	RM2	NR3(2)
14	NR4	RM2(2)
15	NR2(2)	NR3

Tabla 7
Estructuración de pagos para el J_1 (Rusia) y J_2 (Estonia) según comparación de pagos en cada escenario en términos de escenario normativo

	J_1 – Rusia	**J_2 – Estonia**
NR1	4	11
RED1	12	8
RM2	13	3
NR2	5	5
RM2(2)	3	14
NR2(2)	15	1
NR3	9	15
GC3	7	10
RED3	11	7
RM3	2	4
RED3(2)	10	6
RC3	6	9
NR3(2)	8	13
NR4	14	2
RM4	1	12

Nota. Denota la justificación para exhibir un sistema de armas mejorado que genere un efecto disuasorio (Brodie, 2011: 281).

Tomando la reestructuración de los pagos para los jugadores bajo el supuesto de la adopción por parte de Estonia de una estrategia de ciberdisuasión sólida, los resultados de una nueva modelización indican que la ejecución de una campaña rusa en el ámbito cibernético no daría mejores pagos que en circunstancias de responder por la vía diplomática o económica. Tanto la vía militar o el no responder quedan descartados por los costos implícitos existentes para ambos jugadores. En este sentido, si Estonia hubiese tenido mecanismos disuasivos fuertes en el ciberespacio, Rusia probablemente hubiese optado por la vía diplomática/económica (RED1) y hubiese omitido la posibilidad de ejecutar un ciberataque ante la directiva del gobierno estonio de sacar la estatua del Soldado de Bronce.

Habiendo considerado un supuesto escenario donde Estonia contaba con una estrategia de ciberdisuasión operativa, el juego que se desarrolla a continuación presenta la reestructuración de los pagos para los jugadores Rusia y Estonia:

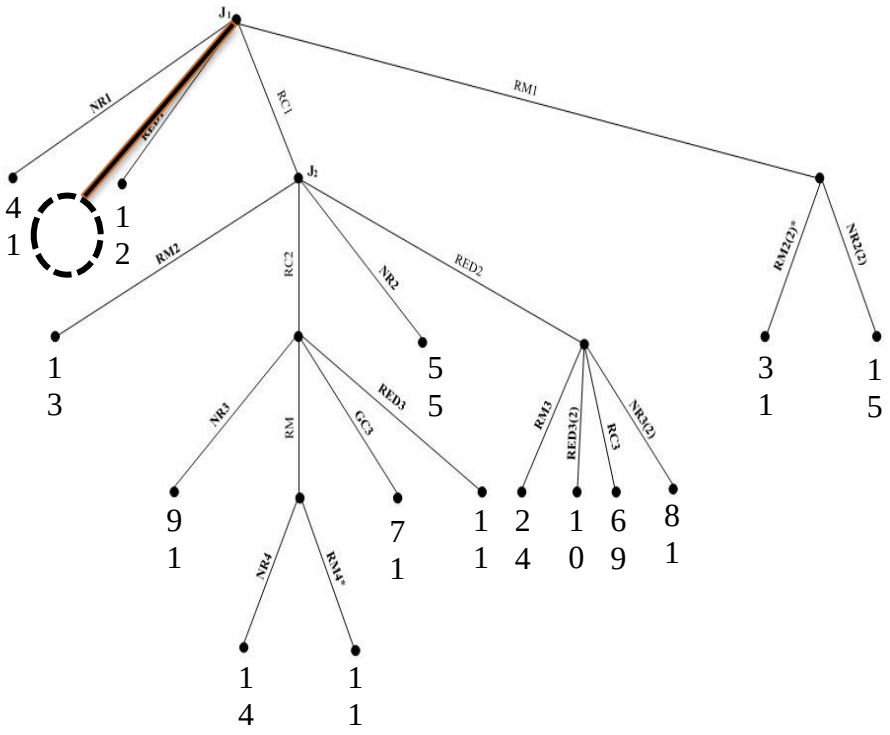

Gráfico 3. Representación gráfica de forma extensiva de escenario normativo

Discusión

En 2007 Estonia sufrió una serie de ataques cibernéticos disruptivos que se prolongó durante poco más de un mes y causó una parálisis a nivel estatal considerando el alto grado de dependencia de Estonia a las redes cibernéticas. El hecho desencadenante fue una directiva del gobierno de Estonia que pretendía sacar la estatua del Soldado de Bronce, ícono de orgullo para los ruso étnicos en Estonia y símbolo de la opresión soviética para los estonios. Estos ataques fueron adjudicados como responsabilidad de Rusia, primeramente, por el gobierno estonio y posteriormente confirmado por un activista del grupo pro-Kremlin Nashi.

Si bien existen varias formas de justificar por qué Rusia intervino, una incógnita que quedó inconclusa fue por qué Rusia eligió ejecutar un ciberataque teniendo a disposición otras demostraciones por la vía militar, por la diplomática o la económica. En estos términos, esta investigación trató de dar una respuesta a tal interrogante.

Los resultados confirman la hipótesis sugerida: la respuesta cibernética por parte de Rusia se dio considerando que las vulnerabilidades de Estonia en el plano cibernético frente a la falta de mecanismos de disuasión ofensivos generaban un esquema de altos beneficios y bajos costos para Rusia. El elemento disuasivo de la OTAN ponía en jaque la plausibilidad de un ataque militar ruso, mientras que la ausencia de reglas claras sobre el ciberespacio en términos de definir lo que se considera un ataque abrieron la posibilidad de un acto ofensivo de bajo costo y altos beneficios. Tal como planteamos en el escenario normativo, si Estonia hubiese tenido mecanismos de disuasión efectivos, Rusia hubiese efectivamente optado por la vía económica/diplomática, considerando que los pagos para las opciones de no responder, responder por la vía cibernética o responder por la vía militar tenían costos mayores.

Ahora bien, aunque hemos comprobado la hipótesis planteada, debe considerarse la existencia de ciertas limitaciones de la investigación llevada a cabo. En primera instancia, algunos datos se basaron en estimaciones de informes de *think thanks* dado que parte de la información requerida resulta confidencial para algunos de los Estados analizados en este trabajo. Por otra parte, la propia teoría de juegos recibe varias críticas: el juego propone una serie de opciones disponibles limitadas que se confinan a la representación extensiva en el árbol de decisiones, mientras que en la realidad, las

opciones son más amplias en términos de grado y variabilidad; segundo, en el juego no se contempla el factor de la incertidumbre, que muchas veces sobrepasa a la posibilidad de tomar una decisión a largo plazo de manera racional; y por último, en algunas instancias los procesos de interpretación del juego para muchos estrategas suele darse en juegos específicos (o sub-juegos) y no en la totalidad del "gran juego" como se plantea desde la teoría porque no todos los sub-juegos tienen la misma relevancia para los actores involucrados (Brams, 2000).

Sin embargo, aún con sus limitaciones, este trabajo expuso el análisis de un evento concreto dentro del ámbito de las Relaciones Internacionales tomando como axis metodológica la teoría de juegos, la cual al día de hoy continúa siendo útil para estudiar el comportamiento de los actores internacionales, más aún en casos de fenómenos novedosos como lo es, sin dudas, la ciberguerra. En estos términos, el análisis que en este trabajo se aplicó al caso de Estonia podría adaptarse para el estudio de otros casos del mismo espacio como por ejemplo el caso de Georgia en 2008, el caso de Stuxnet en 2010 o el de Sony en 2014.

Los acontecimientos ocurridos en Estonia en 2007 resaltaron la necesidad de considerar al ciberespacio como un nuevo campo de batalla. Lejos de cumplirse la premisa de algunos académicos sobre el fin del "paradigma de la disuasión" a finales de Guerra Fría, la ciberguerra hoy se configura como un hecho consumado y la ciber-disuasión, ante este escenario, debe ser un imperativo. Aún en épocas de nuevas tecnologías que han interconectado al mundo, el antiguo adagio realista sigue imponiendo su impronta; *si vis pacem, para bellum.*

Referencias bibliográficas

ALLISON, G. (1971). *Essence of Decision: Explaining the Cuban Missile Crisis*. Little Brown. ISBN 0-673-39412-3.

BARLETTA, W. (2017). *Cyberwar or Cyber-terrorism: The Attack on Estonia*. Cambridge: Massachusetts Institute of Technology.

BENNETT, P. (1995). Modelling Decisions in International Relations: Game Theory and Beyond. *Mershon International Studies Review*, 39:1.

BODMER, M. (2017). Our interconnected world – a force for good?. *Julius Bär*.

BOSTON, S., JOHNSON, M., BEAUCHAMP-MUSTAFAGA, N. y CRANE, Y. (2018). Assessing the Conventional Force Imbalance in Europe: Implications for Countering Russian Local Superiority. *Rand Corporation*.

BRAMS, S. (2000). Game Theory: Pitfalls and Opportunities in Applying It to International Relations. *International Studies Perspectives*, 1, pp. 221-232.

BRODIE, B. (2011). Military Demonstration and Disclosure of New Weapons. *World Politics*, 5:3, pp. 281-301. Recuperado de: http://journals.cambridge.org/abstract_S0043887100018372

CARLINI, A. (2016). Ciberseguridad: un nuevo desafío para la comunidad internacional. *Instituto Español de Estudios Estratégicos*, 67, pp. 950-966.

COMMITTEE ON INTERNATIONAL CONFLICT RESOLUTION (2000). *International Conflict Resolution After the Cold War*. Washington, DC: The National Academies Press.

DAVIS, P., GILMORE, J., FRELINGER, D., et. al. (2019). Exploring the Role Nuclear Weapons Could Play in Deterring Russian Threats to the Baltic States. *Rand Corporation*.

ESTONIAN MINISTRY OF DEFENCE (2011). *National Defense Strategy of Estonia*.

FEAKIN, T. (2015). Developing a Proportionate Response to a Cyber Incident. *Council of Foreign Relations*. Recuperado de: https://www.cfr.org/report/developing-proportionate-response-cyber-incident

FLANAGAN, S. y CHINDEA, I. (2019). Russia, NATO, and Black Sea Security Strategy: Regional Perspectives from a 2019 Workshop. *Rand Corporation*.

GANUZA ARTILES, N. (2011). Situación de la Ciberseguridad en el ámbito internacional y en la OTAN. Instituto Español de Estudios Estratégicos, *Ciberseguridad: retos y amenazas a la seguridad nacional en el ciberespacio* (pp. 165-214). Madrid: Imprenta del Ministerio de Defensa.

GOODMAN, W. (2010). Cyber Deterrence: Tougher in Theory than in Practice?. *Strategic Studies Quarterly*, 4:3, pp. 102-135.

GRIGAS, A. (2012). Legacies, Coercion and Soft Power: Russian Influence in the Baltic States. *Chatam House*.

HAASS, R. (2017). Why The World Needs To Police The Growing Anarchy Of Cyberspace. *Council of Foreign Relations*.

HEATH, (2019). How Estonia became an e-government powerhouse. *TechRepublic*. Recuperado de: https://www.techrepublic.com/article/how-estonia-became-an-e-government-powerhouse/

HERZOG, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, 4:2, pp. 49-60.

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES (2007). *The Military Balance 2007*.

JORDAN, J. (2014). Gestión de la Incertidumbre en las Relaciones Internacionales. *Grupo de Estudios en Seguridad Internacional*. Universidad de Granada.

KYLE, J. (2018). Contextualizing Russia and the Baltic States. *Foreign Policy Research Institute*.

LEE MYERS, S. (2004). As NATO Finally Arrives on Its Border, Russia Grumbles. *The New York Times*.

LOWE, C. (2009). Kremlin loyalist says launched Estonia cyber-attack. *Reuters*. Recuperado de: https://www.reuters.com/article/us-russia-estonia-cyberspace/kremlin-loyalist-says-launched-estonia-cyber-attack-idUSTRE52B4D820090313

MAGUIRE, S. (2019). The Positive Impact of NATO's Enhanced Forward Presence. *The Strategy Bridge*.

MONSALVE, S. (2002). Teoría de Juegos: ¿Hacia dónde vamos? (60 años después de von Neumann y Morgenstern). *Revista de Economía*, Institucional, 7.

MORGENSTERN, O. (1955). La teoría de los juegos y el comportamiento económico. *Económica*, 1:3, pp. 345-375.

MORROW, J. (1994). *Game Theory for Political Scientists*. Princeton: Princeton University Press.

NYE, J. (2011). Cyberspace Wars. *The New York Times*. Recuperado de: https://www.nytimes.com/2011/02/28/opinion/28iht-ednye28.html

NYE, J. (2015). ¿Se puede ejercer la disuasión en la guerra cibernética?. *Project Syndicate*.

OTAN (2011). Financial and Economic Data Relating to NATO Defence. *North Atlantic Treaty Organization*. Recuperado de: https://www.nato.int/nato_static/assets/pdf/pdf_2011_03/20110309_PR_CP_2011_027.pdf

PARK, A. (1994). Ethnicity and Independence: The Case of Estonia in Comparative Perspective. *Europe-Asia Studies*, 46:1, pp. 69-87.

PÉREZ, J., JIMENO, J. S. y CERDÁ, E. (2004). *Teoría de Juegos*. Madrid: Pearson Educación.

SCHMIDT, A. (2013). The Estonian Cyberattacks. Healey, J., *A fierce domain – conflicts in cyberspace 1986-2012*. Washington D.C.: Atlantic Council.

SHLAPAK, D. y JOHNSON, M. (2016). Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics. *Rand Corporation*.

SHLAPAK, D. y JOHNSON, M. (2016). Rethinking Russia's Threat to NATO. *Rand Corporation*.

SINGER, P. y FRIEDMAN, A. (2014). *Cybersecurity and cyberwar: what everybody needs to know*. Nueva York: Oxford University Press.

STONE, R. (2001). The Use and Abuse of Game Theory in International Relations. *Journal of Conflict Resolution*, 45:2.

TRAYNOR, I. (2007). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*.

WALTZ, K. (1990). Nuclear Myths and Political Realities. *American Political Science Review*, 84:3, pp. 731-745.

WALTZ, K. (2000). Structural Realism after the Cold War. *International Security*, 25:1, pp. 5-41.

Notas de pie de página

[i] Son sistemas físicos y virtuales que se consideran esenciales para las operaciones cotidianas entorno a la economía, la seguridad y el bienestar general de las sociedades. Entre ellas se destacan los sistemas de corriente eléctrica, suministro de agua, transporte y comunicación, entre otros.

[ii] Para más información sobre la utilidad de la aplicación de la Teoría de Juegos en las Relaciones Internacionales se recomiendan: Bennett, P. (1995). Modelling Decisions in International Relations: Game Theory and Beyond. *Mershon International Studies Review*, 39:1; Stone, R. (2001). The Use and Abuse of Game Theory in International Relations. *Journal of Conflict Resolution*, 45:2; y Brams, S. (2000). Game Theory: Pitfalls and Opportunities in Applying It to International Relations. *International Studies Perspectives*, 1.

[iii] Véase en el Gráfico 1 las acciones RM2, RM2(2) y RM4.

[iv] Se recomienda leer: Shlapak, D. y Johnson, M. (2016). Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics. *Rand Corporation*; Shlapak, D. y Johnson, M. (2016). Rethinking Russia's Threat to NATO. *Rand Corporation*; Maguire, S. (2019). The Positive Impact of NATO's Enhanced Forward Presence. *The Strategy Bridge*; Davis, P., Gilmore, J., Frelinger, D., et. al. (2019). Exploring the Role Nuclear Weapons Could Play in Deterring Russian Threats to the Baltic States. *Rand Corporation*; Boston, S., Johnson, M., Beauchamp-Mustafaga, N. y Crane, Y. (2018). Assessing the Conventional Force Imbalance in Europe: Implications for Countering Russian Local Superiority. *Rand Corporation*; Flanagan, S. y Chindea, I. (2019). Russia, NATO, and Black Sea Security Strategy: Regional Perspectives from a 2019 Workshop. *Rand Corporation*.

[v] Un ataque ruso convencional contra Estonia hubiese desencadenado una respuesta al Artículo 5 de la OTAN. Sin embargo, las demostraciones digitales de fuerza podrían permitir a los Estados subvertir las restricciones legales del sistema internacional (Herzog, 2011). El ministro de defensa estonio, Jaak Aaviksoo en su momento declaró "En la actualidad, la OTAN no define los ciberataques como una acción militar clara. Esto significa que las disposiciones del Artículo V del Tratado del Atlántico Norte, o, en otras palabras, la autodefensa colectiva, no se extenderán automáticamente al país atacado" (Traynor, 2007).

[vi] Las demostraciones de fuerza son destacadas considerando que están destinadas principalmente a transmitir un propósito y/o una intención o denotar la tenencia de una determinada capacidad. En el primer caso, existen riesgos políticos asociados a las intenciones de realizar una demostración en concreto; en el segundo, tales riesgos en principio no existen, pero sí puede existir una tentación o una