ACTOS INTERNACIONALES EN BARCELONA

Real Academia de Ciencias Económicas y Financieras

LA CIBERSEGURIDAD EN LA CIENCIA Y EN LAS ACTIVIDADES ECONÓMICAS

II SEMINARIO INTERNACIONAL DE PRIMAVERA DE BARCELONA

Barcelona, 24 y 25 de mayo de 2023

LA CIBERSEGURIDAD EN LA CIENCIA Y EN LAS ACTIVIDADES ECONÓMICAS
(II Seminario Internacional de primavera de Barcelona)

La realización de esta publicación
ha sido posible gracias a

MINISTERIO
DE CIENCIA, INNOVACIÓN
Y UNIVERSIDADES

con la colaboración de

Fundación "la Caixa"

con el patrocinio de

Generalitat de Catalunya
Departament
de Justícia

LA CIBERSEGURIDAD EN LA CIENCIA Y EN LAS ACTIVIDADES ECONÓMICAS

(II Seminario Internacional de primavera de Barcelona)

Publicaciones de la Real Academia de Ciencias Económicas y Financieras

Real Academia de Ciencias Económicas y Financieras
"La Ciberseguridad en la Ciencia y en las Actividades Económicas" / Real Academia de Ciencias Económicas y Financieras.

Bibliografía
ISBN- 978-84-09-57484-1

I. Título II. Gil Aluja, Jaime III. Colección

1. Economía 2. Tecnología 3. Transformación

Editora: ©2024 Real Academia de Ciencias Económicas y Financieras, Barcelona.
Fotografía portada: www.freepik.es
Académica Coordinadora: Dra. Ana Maria Gil-Lafuente

ISBN- 978-84-09-57484-1

Depósito legal: B 22391-2023

Obra producida en el ámbito de la subvención concedida a la Real Academia de Ciencias Económicas y Financieras por el Ministerio de Ciencia e Innovación.

Imprime: Ediciones Gráficas Rey, S.L.—c/Albert Einstein, 54 C/B, Nave 12-14-15
Cornellà de Llobregat—Barcelona
Impresión Enero 2024

Esta publicación ha sido impresa en papel ecológico ECF libre de cloro elemental, para mitigar el impacto medioambiental

REAL ACADEMIA DE CIENCIAS ECONÓMICAS Y FINANCIERAS

BARCELONA ECONOMICS NETWORK

SEMINARIO INTERNACIONAL DE PRIMAVERA DE BARCELONA

II EDICIÓN

24-25 DE MAYO DE 2023

"La Ciberseguridad en la Ciencia y en las Actividades Económicas"

ACTO ACADÉMICO

APERTURA Y PRESENTACIÓN PRIMERA JORNADA

Dr. Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras
"Ciberseguridad: mensaje de España al mundo"

PRIMERA SESIÓN ACADÉMICA

Dr. Petre Roman
Miembro de la Barcelona Economics Network
"Incertidumbres y falta de coherencia generadas por la cybersciencia (Inteligencias Artificiales) en la sociedad y en el campo económico en particular"

SEGUNDA SESIÓN ACADÉMICA

Sr. Enrique Lecumberri Matí
Académico de Número de la Real Academia de Ciencias Económicas y Financieras
"Tendencias y desafíos en la ciberseguridad actual: Una mirada desde la perspectiva empresarial"

Dra. Ana Maria Gil-Lafuente
Académica de Número de la Real Academia de Ciencias Económicas y Financieras
"Una revisión Bibliométrica de la investigación sobre Ciberseguridad y negocios, 2004-2022"

TERCERA SESIÓN ACADÉMICA

Dr. Valeriu Ioan Franc
Académico Correspondiente por Rumanía de la Real Academia de Ciencias Económicas y Financieras
"Cyber-Economy, le paradox de la Roumanie"

Dr. Korkmaz Imanov
Académico Correspondiente por Azerbaiyán de la Real Academia de Ciencias Económicas y Financieras
"Interval-Valued intuitionistic fuzzy model for simulation of Azerbaijan national cyber security index"

SEGUNDA JORNADA

Dr. Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras
"Un momento para la memoria de Eugen Simion"

CUARTA SESIÓN ACADÉMICA

Dr. Domenico Marino
Miembro de la Barcelona Economics Network
"Guidelines for the development of cybersecurity economics"

QUINTA SESIÓN ACADÉMICA

Dr. Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras
"Ensayo de un algoritmo para la gestión de la Ciberseguridad"

Dr. Dobrica Milovanovic
Miembro de la Barcelona Economics Network
"Cybersecurity context in Serbia: Legislative and strategic framework"

SÉPTIMA SESIÓN ACADÉMICA

Dr. Carlo Morabito
Miembro de la Barcelona Economics Network
"Deep learning and explainable AI approaches to automatic vulnerability detection and classification for improved cyber-resilience"

Dr. Enrique López González
Académico de Número de la Real Academia de Ciencias Económicas y Financieras
"Finanzas sostenibles en la era del argocapitalismo: el papel de la ciberresiliencia"

OCTAVA SESIÓN ACADÉMICA

Dr. José Daniel Barquero
Académico de Número de la Real Academia de Ciencias Económicas y Financieras
"Economía y ciberdelicuencia cuántica"

Dr. Janusz Kacprzyk
Academico Correspondiente por Polonia de la Real Academia de Ciencias Economicas y Financieras
"Cybersecurity: economic and non- economic aspects"

Dr. Mario Aguer
Académico de Número de la Real Academia de Ciencias Económicas y Financieras
"El humanismo como marco de la actividad empresarial"

CLAUSURA DEL II ACTO INTERNACIONAL DE PRIMAVERA DE BARCELONA

Dr. Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras
"El tratamiento de la subjetividad, un nuevo horizonte para la ciberseguridad"

ÍNDICE

REAL ACADEMIA DE CIENCIAS ECONÓMICAS Y FINANCIERAS

BARCELONA ECONOMICS NETWORK

SEMINARIO INTERNACIONAL DE PRIMAVERA DE BARCELONA
II EDICIÓN

24 - 25 de mayo de 2023

"LA CIBERSEGURIDAD EN LA CIENCIA Y EN
LAS ACTIVIDADES ECONOMICAS"

Apertura y Presentación

Sesión Académica

APERTURA Y PRESENTACIÓN

CIBERSEGURIDAD: MENSAJE DE ESPAÑA AL MUNDO

Presentación

Dr. Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras

La Real Academia de Ciencias Económicas y Financieras en su cruzada hacia una mayor prosperidad compartida, sigue profundizando y ampliando la tarea, que ha hecho propia, de crear una nueva línea de investigación que permita explicar mejor las realidades económicas, cada vez más complejas e inciertas, en las que nos hemos visto inmersos por la rutina de textos y conferencias, reiteradamente repetidos de **corte mecanicista**, con innegable valor formal pero también de innegable inutilidad real. No olvidemos que nuestra tarea última debe permitir el tratamiento de los fenómenos que las nuevas sociedades exigen para alcanzar una convivencia en paz y un creciente bienestar.

Estamos hablado de investigaciones y enseñanzas mecanicistas y, por tanto, desprovistas de aquellos **atributos subjetivos** que definen a un ser vivo como **humano.**

La que con propiedad podríamos llamar "revolución digital", que está cambiando nuestras vidas y que como hemos repetido en muchas ocasiones "ha llegado para quedarse", ha colocado ante nuestros ojos un futuro de **inmensa belleza laboral**, en la que las tecnologías puestas a disposición de los humanos harían más placentero, menos penoso y peligroso y más productivo cada minuto de nuestras vidas.

Ya no es posible aceptar como axioma **de un cuerpo científico** a un sujeto de la actividad económica total y absolutamente **racional**, es decir, desprovisto de todo componente **emotivo**. Entre otras e importantes razones, porque entonces **todos** los humanos tendrían las mismas reacciones ante un mismo fenómeno, sea este una decisión económica o un espectáculo deportivo o teatral.

Nuestra Real Corporación emprendió, hace dos decenios, la tarea de reactivar unas ideas que iniciamos, entre los años 60 y 80 del pasado siglo XX, un grupo de intelectuales, entre los que me encontraba, procedentes de varios países europeos, en Francia y Bélgica, tratando de diseñar desde puntos de vista ideológicos y sociales diferentes, una sociedad futura para hacer frente a lo que se llamaba, por aquel entonces, **desafío tecnológic**o.

Entre ellos se encontraban el ingeniero-matemático francés, Arnorld Kaufmann y el médico homeópata franco-libanés, Jacques Pezé. El grupo se conocía con el nombre de **Quadrivium** y de él solo hemos podido recuperar una obra "La civilisation promotionnelle",[1] y de Jacques Pezé, otra obra elaborada junto a Peter Roche de Coppens, "L'alternance instinctive",[2] que constituyó, según palabras de sus autores, "una llave esencial de la vida". Afortunadamente la biblioteca de la RACEF dispone de una colección importante de las obras de Arnold Kaufmann.

De los retazos que se pudieron recuperar de estos dos genios, son de especial interés a nuestros efectos, los nueve libros publicados por Kaufmann y Gil Aluja, así como los elaborados por este último después del fallecimiento de Kaufmann (1994), por cuanto ya tiene lugar la transición global desde el mecanicismo al humanismo con su generalización del **Principio del tercio excluso** (tertium non datur) mediante el **Principio de simultaneidad gradual,** la incorporación de nuevos conceptos o adaptación de otros envejecidos, como los de "grado" o "nivel", playa de entropía, …, así como la elaboración de una axiomática (siempre incompleta) para la nueva línea de pensamiento económico de carácter humanista, conocida por **Escuela de Economía Humanista de Barcelona**.

1 Quadrivium: "La civilisation promotionnelle". Robert Morel, Les Hautes Plaines de Maine (Francia), 1968.

2 Pezé, J. y Roche de Coppens: "L'Alternance instintive". Editions de l'Aire, 1989 (ISBN : 2-950-2848-1-7)

Se dispone así, hoy, de un cuerpo sólido y coherente capaz de sustentar las más avanzadas investigaciones, incluso más allá del ámbito científico para el que ha sido creado.

Así ha sido hasta ahora, intentando armonizar la elaboración de nuevos conceptos, operadores y métodos por una parte, y de nuevas técnicas, modelos y algoritmos por otra, para su utilización en un amplio abanico de situaciones que las complejas realidades actuales ofrecen.

La elección de los objetos de investigación, en este caso, nos las proporcionan las propias realidades y el pulso que los humanos en sociedad tomamos de ellas. Nos indican sus temores, sus inseguridades y, en definitiva, sus más urgentes necesidades. Nos compete a nosotros buscar la manera de priorizarlas y, sobre todo, buscar el o los caminos a seguir para dar solución a sus carencias.

Nuestro reto consiste en utilizar, de nuestro arsenal científico y tecnológico, aquellos elementos que mejor pueden responder a las informaciones disponibles y a los objetivos a alcanzar.

Somos conscientes de que en cada caso concreto será necesaria una tarea de **adaptació**n. Por ello hemos procurado, siempre, que nuestras técnicas poseyeran las cualidades de **flexibilidad y adaptabilidad.**

Esta es la tarea que hemos llevado a cabo hasta ahora. Son los resultados de ella lo que podemos ofrecer.

En este acto, con el que se inaugura el seminario sobre "La Ciberseguridad en la ciencias y en las actividades económicas", no ha sido difícil priorizar, sobre las demás opciones, el tema ahora escogido: La **ciberseguridad** es una preocupación muy extendida en nuestra sociedad porque atañe tanto a los humanos considerados de manera individual, como en su condición de miembro de diferentes colectividades: empresas, instituciones públicas y pri-

vadas,… ¿Quién no ha sentido el temor de ver vulnerado su intimidad o de ver desaparecer sus 10€ depositados en el banco o ver utilizada su tarjeta de crédito con fines perversos?

Pero la decisión definitiva llegó el pasado 17 de marzo de 2023. A raíz del II Acto Nacional de Castilla-León, con la sesión realizada sobre Ciberseguridad en el **Instituto Nacional de Ciberseguridad**, cuando quedó patente la confluencia de los idearios humanistas del Instituto y de la Real Academia, y la doble vertiente, teoría y realidad, que una colaboración, como la que se planteó, podría potenciar, en gran medida, no solo a las dos instituciones, sino, de manera definitiva, a la sociedad española en el contexto internacional.

En el acto de clausura de la jornada leonesa, ya se pusieron los cimientos de una **axiomática** para el cuerpo científico y técnico de la Ciberseguridad. Ahora es necesario seguir en este camino y con la colaboración de cuantos militamos en el campo de las Ciencias Sociales, transmitir los conocimientos creados para que sean utilizados en las diferentes áreas por los nuevos trabajos digitales.

Lo propusimos en nuestra conferencia de clausura del "Solemne acto conjunto con el Instituto Nacional de Ciberseguridad", el pasado 17 de marzo de 2023: **el futuro será brillante si conseguimos aunar esfuerzos**. Nos anima la esperanza que a este seminario le van a seguir otros muchos, con las variantes que sean necesarias.

Estamos preparados para emprender esta nueva aventura: la docencia impartida nos ha dado el hábito de hablar, el deseo de aprender, la virtud de escuchar. En esto estamos.

Muchas, muchas gracias.

INCERTIDUMBRES Y FALTA DE COHERENCIA GENERADAS POR LA CIBERCIENCIA (INTELIGENCIAS ARTIFICIALES) EN LA SOCIEDAD Y EN EL CAMPO ECONÓMICO EN PARTICULAR

Dr. Petre Roman
Miembro de la Barcelona Economics Network de la Real Academia de Ciencias Económicas y Financieras

Las inteligencias artificiales plantean una serie de amenazas para el "sistema operativo de nuestra civilización", porque su creciente poder sobre el lenguaje significa que llegaría a tener una influencia importante sobre la "tela de la qué está hecha casi toda la cultura de la humanidad".

¿Es que nuestra civilización de hoy se deshace o se reforma bajo las AI? ¿Cuáles son los elementos fundamentales del o de los nuevos „*Pattern*"? Recordemos que somos un sistema complejo y por tanto extremadamente sensible a perturbaciones, incluso las que parecen prácticamente insignificantes, de las condiciones iniciales del sistema. Lo que buscamos, de manera a veces desesperante por ser ya tarde, es la *resiliencia*.

La evidente incapacidad de IA para imaginar el *Punto de inflexión/Umbral crítico*.

Es solo que muy a menudo no hacemos historia en circunstancias de nuestra propia elección, sino en circunstancias creadas por accidentes. No son tan singulares las grandes personalidades que pierden de vista la realidad en momentos cruciales, fiandose desmesuradamente en la universalidad de la razón.

En lugar de proporcionar certeza, existe el riesgo de que introduzcamos algo de lo que no podamos retroceder. Hay muchas consecuencias no deseadas.

Resistir un peligro evidente es vivir bajo un riesgo permanente. La acción es imperativa.

Algunas investigaciones basadas en grandes pruebas/ensayos parecen indicar que ofrecer a las personas información sobre un posible riesgo no cambia significativamente el comportamiento de las personas.

Uno podría pensar que la omnipresencia de las redes sociales y la adicción generalizada a los dispositivos electrónicos conduciría a una mayor cohesión, pero de hecho ha sucedido lo contrario, a pesar del pernicioso dominio de la ciberesfera sobre la imaginación colectiva.

La capacidad de entrelazar partículas sustenta la computación cuántica y la criptografía cuántica. La computación cuántica promete una revolución al proporcionar una forma totalmente nueva de hacer cálculos. La criptografía cuántica ofrece una forma confiable de asegurar las comunicaciones y podría formar la base de una Internet cuántica.

Las computadoras cuánticas pueden explotar las propiedades inusuales de la física cuántica para acelerar los cálculos necesarios. Harán obsoletas las técnicas de encriptación actuales, pero no tan pronto, tal vez décadas. Por ahora, los algoritmos de encriptación pueden continuar descifrando mensajes. Cada día que no actuamos, estamos entregando más datos de usuarios a los atacantes. Pero, ¿no serían los humanos que manejan IA como herramientas los que terminarían teniendo el control? Algunos investigadores de IA están descuidando las responsabilidades éticas y traicionando la confianza pública. En este campo se acumulan incertidumbres que me hacen pensar en lo que solían decir los griegos de Aristoteles: “Lo mejor que puedes esperar es evitar lo peor”

En realidad, hicimos lo que esperaban los ciberterroristas: les ofrecimos mucho espacio libre; incluso los alentamos mediante el uso de su campo de especialización en el *interés del estado*.

El individualismo moderno ha desarrollado aspectos positivos, como la conquista de la autonomía. Pero también negativos, como el predominio de uno mismo sobre los demás. El ser humano es, por un lado, egocéntrico: debe

defenderse, alimentarse y pensar en sí mismo; pero también está abierto a los demás, es comunitario, está el amor… El egocentrismo debe reducirse al mínimo vital de conservación. La fraternidad es algo capital.[1]

La fraternidad y la convivencia están centradas en la fuerza de la vida. Las amenazas en la fuerza del mal.

Comparto, por lo tanto soy / I share, therefore I am parece ser el nuevo mantra. Pero también la tecnología nos hace olvidar lo que sabemos de la vida. Gradualmente, estos lazos se cimentan en un hábito.

Si bien los pioneros de la IA, como Alan Turing, ya advirtió en 1950[2], que deberíamos ser conscientes que "las máquinas pueden tomar el control", muchos investigadores contemporáneos minimizan esta preocupación.

Las IA permiten que las computadoras procesen y generen lenguaje humano. Están capacitados en grandes cantidades de datos utilizando técnicas que van desde enfoques basados en reglas hasta modelos estadísticos y de aprendizaje profundo *(machine-learning)*. Para todos los modelos, excepto los más simples, sus operaciones internas son opacas: no hay una comprensión significativa de cómo generan resultados aparentemente inteligentes y similares a los humanos en una amplia gama de tareas. Los modelos de lenguaje de IA plantean riesgos para los derechos humanos, la privacidad, la equidad, la solidez, la seguridad y la protección. Los modelos de lenguaje de IA pueden ayudar a los actores malos a manipular opiniones a gran escala y automatizar la información errónea y la desinformación de una manera que puede amenazar los valores democráticos.

ChatGPT, un chatbot de inteligencia artificial de la empresa IA abierta de San Francisco, se ocupa de la creación de mitos y la exageración, y sus representantes presentan los productos de la empresa como la primera etapa de la "inteligencia general artificial", o la conciencia equivalente a la humana. Insiste en difundir la idea de que la IA podría transformar fundamentalmente a la humanidad y posiblemente incluso destruirla. En cierto sentido es una

estafa. OpenAI ha inventado un problema que promete resolver, si le pagan, por supuesto.

La mayoría de los científicos en el campo de la IA dice que ChatGPT está lejos de ser una inteligencia equivalente a la humana. La inteligencia artificial general todavía se encuentra en el ámbito de la ciencia ficción y, francamente, siempre puede estarlo. ChatGPT, la aplicación basada en la inteligencia artificial (IA), se está haciendo muy popular. Esta tecnología ofrece grandes ventajas por su capacidad de elaborar con rapidez casi cualquier tipo de documento. Pero también es capaz de generar contenidos totalmente falsos que pueden dañar la reputación de las personas. A nosotros nos empujan hacia una tierra desconocida pensando en los hábitos que se han acumulado en siglos e incluso milenios.

El problema con la inteligencia artificial contemporánea es que no es transparente para el usuario. Ese es un gran problema social. Los medios de comunicación se han convertido en un campo de batalla para controlar la atención humana. Con la nueva generación de IA, el frente de batalla está pasando de la atención a la intimidad. En las próximas décadas podríamos encontrarnos viviendo dentro de los sueños de una inteligencia alienígena. El miedo a la IA ha perseguido a la humanidad solo durante los últimos años.. Pero durante miles de años, los seres humanos han sido perseguidos por un miedo mucho más profundo. Siempre hemos apreciado el poder de las historias y las imágenes para manipular nuestra mente y crear ilusiones. En consecuencia, desde la antigüedad los humanos han temido quedar atrapados en un mundo de ilusiones. Algunos llaman a la IA una “nueva arma de destrucción masiva” que puede aniquilar nuestro mundo mental y social. Es por eso que la primera regulación necesaria es obligar a la IA a revelar que es una IA antes de que lleguemos a un punto de inflexión/umbral crítico.

Necesitamos aprendizaje colectivo sobre lo que la humanidad ha creado, cómo gobernarlo y cómo garantizar que habrá responsabilidad por la creación y el uso de nuevas herramientas.

O humanidad y fraternidad o robotización no tiene sentido. El si o si, o-o u ni-ni golpea y para el pensamiento en este caso.

"Es inquietantemente fácil aprender a hackear", dice el cyber-abogado Scott Shapiro (New Scientist, mayo,2023). Debemos enseñar a las personas a comprender cómo se almacena, manipula, transfiere y, en última instancia, explota la información. Existen muchas soluciones técnicas para mejorar la ciberseguridad, pero no existe una forma técnica de lograr una ciberseguridad perfecta.Aunque solo queramos mejorar la ciberseguridad, en lugar de perfeccionarla, es un error pensar que la forma de hacerlo es a través de medios técnicos. "Es principalmente un problema humano" .Tenemos que centrarnos en los factores sociales, legales, económicos y psicológicos que impulsan, alientan y permiten el comportamiento antisocial, disruptivo e ilegal, comportamientos de piratas informáticos. La ciberseguridad es mucho mejor de lo que solía ser, pero los ataques también son mucho mejores de lo que solían ser. Un ejemplo significativo es que tres piratas informáticos, que lanzaron un malware llamado Mirai, consiguieron tomar el control de dispositivos conectados a Internet de las cosas, como cámaras de seguridad y tostadoras inteligentes. En lugar de ser encarcelados, recibieron cinco años de servicio comunitario, tiempo durante el cual trabajaron para el FBI y ayudaron a detener a un grupo de piratas informáticos del estado-nación. Fueron asesorados por el agente del FBI que los atrapó. El agente especial los desvió hacia una actividad socialmente productiva en lugar de una actividad socialmente derrochadora como ponerlos en la cárcel. Los ciberdelincuentes no quieren hackearte, quieren ganar dinero. Recientemente se ha desarrollado lo que se llama *de-risking*. Pero este intento de reducir los riesgos puede introducir aún más opacidad en el sistema financiero global. El hecho de eliminar prácticamente las relaciones de las cuentas puede agredir las entidades y las personas hacia canales que son menos o simplemente no-regulados canales de trabajo, ángulos oscuros, que no son más difíciles controlar.

Global Behavior and Cultural Code in Complex Systems

Some AI researchers are neglecting ethical responsibilities and betraying the public trust. Fear of AI has haunted humankind for only the past few decades. But for thousands of years humans have been haunted by a much deeper fear. Since ancient times humans have feared being trapped in a world of illusions. Some call AI a "new weapon of mass destruction" that can annihilate our mental and social world. Alan Turing cautioned us at the very beginning of the computer era that we should expect "machines to take control". "The view that machines cannot produce surprises is due to an error of thought... Namely, the assumption that as soon as a fact is presented to us, all its consequences play out immediately and simultaneously in our minds. It's a very useful assumption in many circumstances, but we forget too easily that it's false" [3]. Many real situations in our so-called developed world of today are testimonies of the numerous crises that result when an "atmosphere of fear interacts with the logic of law enforcement, which holds that quick-trigger use of force is always justified by what might have happened" [4]. What kind of interaction is this? An unexpected one or a new normal? Let's remember Cicero's homo novus and ask if what happened then, when "personal interests united people against public interests and implacably hostile enemies as of yesterday, were found the next day, shoulder to shoulder, on the same bench, as best friends", is a human behavior unchanged two millennia later [5]. Edgar Morin says that man is "foolish-wise" and therefore, "it is a question of asking whether the progress of complexity, ingenuity, intelligence, and society have been made despite, with or because of disorder, error or fantasy. And we will respond because of, with and despite at the same time; the right answer can only be complex and contradictory" [6]. It is then appropriate to think that the health of social and economic systems can be ensured by a mixture between, on the one hand, feedback and regulations and as much flexibility as possible, and room for creativity, innovation and adaptation to new conditions, on the other hand. This would be what would be the dynamics of complex systems at the edge of chaos. The term is borrowed from biology where it designates a critical point very similar to the critical threshold in physics. That dynamic is in fact

a competitive struggle, very similar to the Darwinian selection, to eliminate all possible scenarios which are unfit before it is too late to build or rebuild resilience. Complex systems are everywhere and very different, from atmosphere to ecosystems, optimization problems or behavior of community living beings or artificial networks. Giorgio Parisi, founder of complex systems theory (Nobel Prize for Physics in 2022), has underlined that: "Criticality is not uncommon in biological systems made up of many interacting components[7]. Being critical is a way for the system to be always ready to optimally respond to an external perturbation.

"We have, on the one hand, life experience taken over and assimilated and established in society as norm and, on the other hand, experience gained from real life events, unlived yet. Norm and chance follow each other rather chaotically. The duration of validity of a norm and the moment of occurrence of the random event are unpredictable. However, norms and events coexist in our consciousness" [8]. I would now use conviviality instead of coexistence. Stuart Kauffman, from the perspective of mathematical biology of self-organization , also believes that it is something in-between: "I suspect that the fate of all complex adaptive systems in the biosphere—from cells to the economy—is to evolve toward a natural state between order and chaos, a great trade-off between structure and surprise" [9]. I think he should have not disregarded the important contribution to organization of the above mentioned energies, along with self-organization as a highway. Moreover, culture is a generative system which is functioning with those energies intertwined to power artistic or scientific prowess. Culture is a system of high complexity while hubris, a permanent source of disorder and low complexity, could collapse it to a low level. "The cultural code maintains the integrity and identity of the social system, ensures its auto perpetuation or its invariant reproduction, protecting it from uncertainty, chance, confusion, disorder", says Edgar Morin [10]. This kind of movement to a cultural edge of chaos could display - why not? - the critical threshold feature in its dynamics. How far are we now, at the moment of analysis, from the internal moment of reaching the critical threshold in the system? At least from the moral perspective.

One example from financial matters is interesting. The idea that inflation at 2 percent annually, not, say, 4 percent, is the appropriate inflation target viewed as a consensus today. "The analytical and empirical basis for that consensus is quite weak" says Paul Krugman (Nobel Prize for Economy) [11], but central bankers have come to view restoring 2 percent as a test of their credibility. Anti-inflation policies are always damaging new investments but high inflation is a shocking source of uncertainty. Due to global unpredictability, high correlations between the use of different economic instruments and their consequences are not known. The story could be one of solid resilience or vast pain. The process of modeling the surrounding world, as suggested in the present article, is a process of approximation, in which uniqueness and essentialization are the characteristic traits that stay permanently in the realm of the fundamental results in science. In pragmatic terms, the process is somewhere in-between. "An approximate reasoning system provides something of middle ground between what is explicit or evident and can be retrieved using few resources and what is implicit and should be inferred given enough time and memory" [12]. The results we achieve by approximation as a method/system are part of speculative thinking and are not the approximative thinking which produces unintelligent, unfulfilled or unfinished realities. Speculative thinking is indeed an instrument to grasp facts of nature and life although sometimes it can overestimate improbable situations. In this case we are under a profound psychological effect. Maurice Allais (another Nobel Prize for Economy), who invented the paradox bearing his name, said this effect shows "(the human) preference for safety in the vicinity of certainty" [13].

The psychological state of humanity can't be a stable equilibrium but rather a swinging, beautiful if not perfect, between the will to belief and the obligation to doubt. It's the economic way of thinking. It's the disciplined thinking that is capable of eliminating the variability of expertise, so harmful at the moment of taking decisions based on expertise. The relationship between epistemology, in which the first condition is to define knowledge, and uncertainty is, indeed, subject to the fundamental relationship between attempts to theoretically model perceived reality and the observability of the

universe. A philosophical system is "stable" if it is not only consistent, but if any of its theses does not create insuperable difficulties vis-à-vis other theses of the system. Naturally, the same should be valid in interdisciplinarity. Its truth value is dependent on facts which could lie beyond empirical evidence. The instability of the philosophical system comes from its "effort to both naturalize mathematical knowledge and to assume the bivalence of truth and Gödel's proof that mathematics does not consist in probability but in relation to mathematical facts" says Joseph Vidal-Rosset [14].

We undoubtedly need explanations as intuitive as possible. The clash between logic and intuition needs to be overcome at the moment of decision-making, I e. of synthesis. Otherwise we burden ourselves with a new, possible, uncertainty. Let us keep in mind that uncertainty is the great enemy of action. That is why our action is meant to build resilience to deal better with unpredictable events and prevent the emergence of a critical threshold. Resilience is not built in order to avoid risks. In fact, in the economy, absorbing risks is an imperative as it shows the way to economic progress. Many issues in logic today are no longer about zero-agent notions like truth, or single-agent notions like proof, but rather about processes of verification, argumentation, communication, or general interaction to define our priorities and decisions. And encourage a longer time-perspective, thinking within the past, present and future.

What is the connection to real life? is the question in an attempt to make a connection with what we actually experience. In our society the event (accident) occurs when:

- we don't know how things work (we don't know the rules);
- we do not pay full attention and therefore do not calculate with the necessary accuracy;
- we interact with people who affect our own lives.

Note that this model includes the randomness defined basically in three ways: absence of rules, sensitivity to initial conditions, and external complexity.

Kolmogorov did not think that every event has a probability. In 1951, in his article on probability in the Great Soviet Encyclopedia he is explicit: "Certainly not every event whose occurrence is not uniquely determined under given conditions has a definite probability under those conditions. The assumption that a definite probability (i. e. a completely defined fraction of the number of occurrences of an event if the conditions are repeated a large number of times) in fact exists for a given event under given conditions is a hypothesis which must be verified or justified in each individual case".

Methods, validity, and scope of natural sciences presupposes choice in accordance to social needs; it must follow the fundamental problems we face. According to the empirical evidence in environmental sciences as shown by Nearing and al. [15], these problems are:

- The problem of the finite number of experiments;
- The problem of the finite number of hypotheses;
- The problem of being able to test sets of hypotheses rather than individual hypotheses.

Conclusion

Social media has become a battleground for controlling human attention. Vast amounts of energy, time and capital are devoted to creating imaginary universes. With the new generation of AI, the battlefront is shifting from attention to intimacy. In the coming decades we might find ourselves living inside the dreams of an alien intelligence. AI offers a risk-averse landscape selling to the global audience very questionable values. The risks are high entering a poor cultural and moral territory. Maybe changing the whole orbit of thinking.

Referencias

[1] Edgar Morin, “Method”, Volume 1, “The Nature of Nature”, Ed. Peter Lang, 1992, p. 13.

[2] A. M. Turing, “Computing Machinery and Intelligence”, Mind, 49, 1950, pp. 433-460.

[3] ibidem [2]

[4] Rachel Bedard, “A Culture of Repression and Neglect“, NYRB, 11 May 2023.

[5] Quoted in N. I. Barbu, “Scrisorile lui Cicero” (Cicero’s letters), in Romanian, Editura Academiei R. P. R., 1959, p. 38.

[6] Edgar Morin, “Le paradigme perdu: la nature humaine”, Éditions du Seuil, 1973, , p. 174, p. 173

[7] Giorgio Parisi, interview with Ginestra Bianconi, Journal of Physics: Complexity, 12th January 2023.

[8] Petre Roman, “We Live Under the Permanent Conviviality of Norms and Chance--Understanding It Is Key to Building More Resilient Complex Systems”, International Journal of Philosophy, Vol. 10, No. 4, 2022, pp. 147-152.

[9] Stuart A. Kauffman, “The Origins of Order: Self-organization and Selection in Evolution”, Oxford University Press, 1993, p. 181. (53)

[10] ibidem [6]

[11] Paul Krugman, “ How Low Must Inflation Go?”, New York Times, June 9, 2023

[12] Eric Pacuit, “Logics of Informational Attitudes and Informative Actions”, Journal of Indian Center of Philosophical Research, Volume XXVII, Number 1, January-March 2010.

[13] Maurice Allais, “The So-called Allais Paradox and Rational Decisions Under Uncertainty”, in “Expected Utility Hypotheses and the Allais Paradox”, Allais et Hagen, editors, 1979.

[14] Joseph Vidal-Rosset, “Does Gödel’s Incompleteness Theorem Prove That Truth Transcends Proof ?”, Researchgate.net/publication/226670228, January 2006.

[15] G. S. Nearing, Y. Tian, H. V. Gupta, M. P. Clark, K. W. Harrison, S. V. Weijs, “A philosophical basis for hydrological uncertainty”, Hydrological Sciences Journal, vol. 61, 2016, pp. 1666-1678.

TENDENCIAS Y DESAFÍOS EN LA CIBERSEGURIDAD ACTUAL: UNA MIRADA DESDE LA PERSPECTIVA EMPRESARIAL

Sr. Enrique Lecumberri Matí
Académico de Número de la Real Academia de Ciencias Económicas y Financieras

Abstract:

La ciberseguridad se ha convertido en una de las mayores preocupaciones de las empresas en todo el mundo.

En un entorno cada vez más digitalizado, las organizaciones se enfrentan a una gran cantidad de amenazas que pueden afectar gravemente su funcionamiento y poner en riesgo la información confidencial de sus clientes. En este artículo de investigación se analizan las principales tendencias y desafíos en el ámbito de la ciberseguridad desde la perspectiva empresarial.

Se hace una revisión de las amenazas más comunes que enfrentan las organizaciones en la actualidad, tales como el phishing, el ransomware y los ataques de ingeniería social, así como de las técnicas y herramientas que se utilizan para prevenir y mitigar estos ataques.

Se hace especial hincapié en la importancia de la concienciación y la formación de los empleados en materia de ciberseguridad, así como en la necesidad de adoptar medidas preventivas y de respuesta ante posibles incidentes.

Se analizan también las implicaciones legales y regulatorias de la ciberseguridad, incluyendo la normativa europea sobre protección de datos (GDPR) y la directiva NIS sobre seguridad de las redes y sistemas de información.

I

“En el mundo digital actual, la ciberseguridad es la virtud que nos permite salvaguardar nuestros bienes más valiosos: nuestros datos y nuestra privacidad”.

Este enunciado hace referencia al concepto de virtud en la filosofía griega, específicamente en la obra de Platón. Según Platón, las virtudes son cualidades esenciales que permiten a una persona vivir una vida plena y justa. De manera similar, en el mundo digital, la ciberseguridad es una virtud esencial que permite a los individuos y las empresas protegerse contra los riesgos y las amenazas que pueden poner en peligro su privacidad y sus datos.

Así como la virtud en la filosofía griega requiere una práctica constante y la toma de decisiones conscientes, la ciberseguridad también requiere una actitud proactiva y la implementación de medidas adecuadas para protegerse contra los riesgos informáticos. En un mundo donde la tecnología y la información son cada vez más valiosas, la ciberseguridad se ha convertido en una virtud fundamental para proteger nuestros bienes más valiosos.

Es por tanto un axioma de este siglo XXI d. C. que la transformación digital ha supuesto una revolución en el mundo empresarial, permitiendo la automatización de procesos, la reducción de costes y la mejora de la eficiencia. Sin embargo, esta digitalización y la hiperconectividad de la sociedad también ha traído consigo una serie de riesgos en materia de seguridad, que pueden afectar seriamente a las empresas y a sus clientes. Las amenazas en el ámbito de la ciberseguridad son cada vez más sofisticadas y están en constante evolución, por lo que es fundamental que las empresas se mantengan al día en materia de seguridad para poder prevenir y mitigar posibles ataques.

En concreto, el Foro Económico Mundial, no repara en indicar que el 86% de los líderes empresariales y el 93% de los expertos del sector esperan inestabilidad geopolítica que, en el plazo de dos años, podría dar lugar a un evento de ciberseguridad de resultado catastrófico para las organizaciones y

las democracias avanzadas del mundo[1]. Cabe destacar además que, para la organización internacional mencionada encargada de la cooperación público-privada, los riesgos de ciberseguridad están en el puesto número 8 de los mayores riesgos del mundo a los que se enfrentan las sociedades hoy en día, y en el mismo listado de problemas tan relevantes como el cambio climático, confrontaciones geoeconómicas, desastres naturales o migraciones involuntarias a gran escala.

II
Amenazas y desafíos actuales en ciberseguridad

En la última década, las amenazas cibernéticas han evolucionado significativamente. Desde el **phishing** hasta el **malware** y el **ransomware**, las tácticas utilizadas por los ciberdelincuentes son cada vez más sofisticadas y efectivas. La divulgación no autorizada de información, el engaño por medios electrónicos, la protección de la información personal y la incapacidad para acceder a servicios pueden crear problemas de seguridad para los usuarios, ya que pueden violar sus derechos, libertades y hasta poner en riesgo su vida.

Cada año, la agencia europea para la ciberseguridad (ENISA) produce un informe que presenta las principales amenazas a la seguridad informática en diversas industrias. El informe más reciente, publicado en noviembre de 2022, también destaca los sectores que se ven más afectados por los impactos digitales relacionados con la privacidad, la integridad y la disponibilidad de los sistemas. En este sentido, el informe indica que los gobiernos y la administración pública son los más vulnerables, seguidos por sectores como servicios, proveedores de servicios digitales, finanzas, energía y salud.

El servicio de reclamaciones del Banco de España del año 2022 señala que en los expedientes analizados durante 2021 se observó el aumento de reclamaciones en las que intervienen técnicas empleadas por ciberdelincuentes,

1 Perspectivas de ciberseguridad global para 2023, Foro Económico Mundial.

como el phishing (por correo electrónico), vishing (de forma telefónica) o el smishing (vía sms). Mediante estas técnicas los ciberdelincuentes se hacen pasar por las entidades financieras o incluso por organismos públicos o empresas de reconocida trayectoria, suplantando su identidad y pidiendo a las potenciales víctimas que facilien, después de clicar en un enlace –aparentemente genuino, pero en realidad malicioso- determinados datos personales y bancarios.

Las siguientes son algunas de las principales amenazas cibernéticas que han surgido en los últimos años[2]:

Phishing
El phishing es una técnica en la que los delincuentes cibernéticos envían correos electrónicos fraudulentos a los usuarios para obtener información confidencial. Esta técnica se ha vuelto cada vez más sofisticada y los ciberdelincuentes utilizan técnicas de ingeniería social para hacer que los correos electrónicos parezcan legítimos y persuadir a los usuarios para que proporcionen información confidencial.

Malware (también denominados virus informáticos)
El malware es un tipo de software malicioso que puede infectar sistemas y dispositivos, robar información o incluso tomar el control total del dispositivo infectado. Los ciberdelincuentes utilizan diferentes tipos de malware, como virus, troyanos y spyware, para atacar sistemas y robar información.

Ransomware
El ransomware es una forma de malware que cifra archivos o sistemas completos, bloqueando el acceso del usuario. Los ciberdelincuentes exigen un rescate para proporcionar una clave de descifrado para liberar el sistema o los archivos afectados.

2 Fuente: Informe del estado de la ciberseguridad 2022, asociación ISACA

Ingeniería social

Los ataques de ingeniería social son una técnica en la que los delincuentes utilizan información personal y engañan a los usuarios para que divulguen información confidencial. Estos ataques pueden incluir la suplantación de identidad o el envío de correos electrónicos fraudulentos.

La automatización robótica de procesos

Si bien la automatización robótica de procesos puede aportar beneficios significativos a las organizaciones como mejorar la eficiencia y reducir costes, también existen riesgos asociados con su implementación que deben considerarse, a saber: la falta de control y supervisión, la dependencia de proveedores que podría limitar la flexibilidad y adaptabilidad de la organización ante cambios tecnológicos o de negocio, la resistencia al cambio y desplazamiento laboral, o la securización al acceso / procesamiento y almacenamiento de información sensible, pudiendo generar problemas a cualquier organización que explore dichos procesos automatizados.

Noticias falsas (también conocidas como "fake news")

Tiene como objetivo publicar información falsa o incorrecta a través de fuentes públicas y redes sociales, con el fin de influir en las opiniones y el pensamiento de la sociedad. A pesar de que los periódicos digitales son una fuente comúnmente utilizada para obtener noticias, existen plataformas digitales como redes sociales y foros de opinión donde se puede difundir información sin un adecuado esfuerzo de contraste, lo que puede llevar a noticias falsas o manipuladas a ser publicadas en periódicos digitales reconocidos, lo que aumenta su credibilidad. En ocasiones, este tipo de noticias pueden estar exageradas con el objetivo de atraer lectores y generar más tráfico en sus sitios web, y también puede llevar a que los algoritmos automáticos elijan noticias con mayor tráfico para colocarlas en posiciones más visibles, sin una adecuada verificación de la información. La reciente invasión de Ucrania por parte de Rusia, ha demostrado nuevas formas de utilizar estas amenazas para cambiar la percepción del público

sobre la guerra y la responsabilidad de las partes involucradas, por poner un ejemplo y el impacto real que pueden llegar a generar.

Además, cobra especialmente importancia un nuevo parámetro, la **Inteligencia Artificial (IA)**, ya que si bien puede ser utilizada para proteger el mundo empresarial (o incluso ayudar en la elaboración del presente artículo), los atacantes de una organización cuentan con la IA con mayores capacidades de automatización para ocasionar cualquier tipo de problema, mayores capacidades de programación y búsqueda de vulnerabilidades o incluso de creación de escenarios lógicos a los cuales muchas organizaciones podrían sucumbir.

Sin llegar a citar todas las amenazas posibles, en este contexto anteriormente descrito, es importante entrar a destacar varios desafíos actuales en ciberseguridad empresarial, entre los cuáles los más importantes podrían ser los siguientes:

Falta de concienciación y formación de los empleados: La mayoría de los ataques cibernéticos tienen éxito debido a la falta de concienciación y formación de los empleados en materia de ciberseguridad. Los empleados son la primera línea de defensa contra los ataques cibernéticos, por lo que es fundamental que estén bien informados y capacitados para detectar y prevenir posibles amenazas[3].

Los empleados deben ser informados sobre las amenazas informáticas comunes y capacitados para detectar y prevenir los ataques informáticos. Se debe construir para ello un plan de formación con los temas a tratar, comunicar la política de seguridad, realizar programas específicos para los diferentes grupos de empleados, incentivar la cultura de ciberseguridad y, por supuesto, evaluar su rendimiento que permitan identificar si hay que mejorar o no la metodología empleada.

3 Fuente: Addressing the EU cybersecurity skills shortage and GAP through higher education, Agencia de la Unión Europea para la Ciberseguridad (ENISA)

Falta de especialistas

Hay varias razones para la falta de especialistas en seguridad informática en la actualidad. Algunos de los factores clave incluyen:

- Demanda creciente: A medida que la dependencia de la tecnología aumenta en todos los aspectos de la vida, la demanda de profesionales en seguridad informática ha crecido rápidamente. Las organizaciones de todos los tamaños y sectores necesitan expertos en seguridad para proteger sus sistemas y datos, lo que ha creado una escasez de talento en el mercado.

- Evolución constante de las amenazas: Las amenazas cibernéticas están en constante evolución, y los delincuentes cibernéticos buscan constantemente nuevas formas de infiltrarse en los sistemas y robar información. Esto requiere que los profesionales de seguridad se mantengan actualizados sobre las últimas técnicas y herramientas de ataque, lo que puede resultar desafiante para mantenerse al día.

- Brecha de habilidades y conocimientos: La seguridad informática es un campo altamente especializado que requiere una combinación única de habilidades técnicas y conocimientos en áreas como redes, criptografía, análisis forense, gestión de incidentes y cumplimiento normativo. La falta de programas educativos y de capacitación específicos en seguridad informática ha contribuido a una brecha de habilidades en el mercado laboral.

En cuanto a los perfiles que más escasean en seguridad informática, algunos de los roles más demandados son:

- Analistas de seguridad: Estos profesionales son responsables de monitorear y analizar las amenazas de seguridad, investigar incidentes, implementar medidas de mitigación y realizar pruebas de penetración.

- Ingenieros de seguridad: Estos especialistas se encargan de diseñar, implementar y mantener las infraestructuras de seguridad de una organización, incluyendo firewalls, sistemas de detección y prevención de intrusiones, y soluciones de gestión de identidad y acceso.

- Especialistas en seguridad en la nube: Con el aumento de la adopción de servicios en la nube, los profesionales con habilidades en seguridad en entornos de nube son muy solicitados. Estos expertos se enfocan en proteger los datos y las aplicaciones que residen en plataformas de servicios en la nube.

- Expertos en análisis forense digital: Estos profesionales investigan y recolectan evidencia digital relacionada con incidentes de seguridad, colaboran en investigaciones legales y ayudan en la recuperación de sistemas comprometidos.

- Consultores de seguridad: Los consultores de seguridad brindan asesoramiento y recomendaciones a las organizaciones sobre cómo mejorar su postura de seguridad, evaluar riesgos y cumplir con los estándares y regulaciones aplicables.

Estos son solo algunos ejemplos de los perfiles más escasos en seguridad informática, pero en general, la demanda supera con creces la oferta en la mayoría de las áreas de especialización en este campo.

Por otra parte, existen varias razones por las cuales los empleados de las empresas pueden estar mal entrenados en el ámbito de la ciberseguridad:

- Falta de conciencia: Muchos empleados no tienen un nivel adecuado de conciencia sobre las amenazas cibernéticas y los riesgos asociados. Pueden subestimar la importancia de seguir prácticas de seguridad o no entender cómo sus acciones pueden afectar la seguridad de la empresa.

- Capacitación insuficiente: Algunas organizaciones no brindan suficiente capacitación en ciberseguridad a sus empleados. Pueden considerar que no es una prioridad o no disponen de los recursos necesarios para ofrecer una formación adecuada.

- Falta de actualización: Las amenazas y las técnicas de ataque evolucionan constantemente, lo que requiere que los empleados estén actualizados y capacitados en las últimas tendencias de seguridad. Si las empresas no proporcionan una formación continua, los empleados pueden quedarse rezagados en términos de conocimientos y habilidades.

- Complejidad de la tecnología: La tecnología y los sistemas de información están cada vez más interconectados y son cada vez más complejos. Esto puede dificultar la comprensión de los empleados sobre cómo operan los sistemas y cómo pueden protegerlos adecuadamente.

En cuanto a los errores más comunes cometidos por los empleados en el ámbito de la ciberseguridad, algunos de ellos incluyen:

- Uso de contraseñas débiles: Muchos empleados utilizan contraseñas débiles o las comparten con otros, lo que facilita el acceso no autorizado a sus cuentas y a los sistemas de la empresa.

- Phishing y ingeniería social: Los ataques de phishing y la ingeniería social se basan en engañar a los empleados para que revelen información confidencial o hagan clic en enlaces maliciosos. La falta de conciencia puede llevar a que los empleados caigan en estas trampas.

- Descuido con los dispositivos y la información: Los empleados pueden dejar dispositivos desbloqueados o sin supervisión, lo que facilita el acceso no autorizado a la información. También pueden ser descuidados al desechar documentos físicos o digitales confidenciales.

- Falta de actualizaciones de software: No mantener el software y los dispositivos actualizados con los últimos parches de seguridad puede dejarlos vulnerables a ataques conocidos.

- Uso no autorizado de dispositivos y aplicaciones: Los empleados pueden conectar dispositivos personales no autorizados a la red de la empresa o utilizar aplicaciones y servicios no aprobados, lo que puede introducir riesgos de seguridad.

Escasez de talento en ciberseguridad: Existe una gran demanda de profesionales capacitados en ciberseguridad, pero hay una escasez de talento en este campo. En concreto, 3,4 millones de profesionales[4]. Esto hace que sea difícil para las empresas encontrar y retener a los expertos en ciberseguridad que necesitan para proteger sus sistemas y datos. Y no sirve cualquier experto, sino aquellos que tienen las capacidades técnicas, junto con otras características de comportamiento o capacidades intangibles, que les capacitan para un trabajo tan específico, para poder desarrollar el trabajo con altas dosis de creatividad, con una fuerte componente de comunicación y que puedan trabajar con otros profesionales en equipo.

Aumento de los ataques cibernéticos sofisticados: Los ataques cibernéticos están en constante evolución y cada vez son más sofisticados y difíciles de detectar. Los atacantes utilizan técnicas avanzadas para burlar las medidas de seguridad, lo que hace que sea cada vez más difícil protegerse contra ellos.

Brechas de seguridad en proveedores de servicios en la nube: Cada vez más empresas están utilizando servicios en la nube para almacenar y procesar sus datos, lo que puede exponerlos a riesgos de seguridad adicionales. Las brechas de seguridad en los proveedores de servicios en la nube pueden tener consecuencias graves para las empresas, ya que pueden resultar en la pérdida de datos confidenciales o la interrupción del negocio[5].

4 Fuente: Cybersecurity Workforce Study, asociación (ISC)2

5 Fuente: Data Loss Prevention and Data Security Survey Report 2023, Cloud Security Alliance (CSA).

Cumplimiento regulatorio: Las empresas están sujetas a una serie de regulaciones y leyes en materia de ciberseguridad, como la GDPR y la directiva NIS (ver más adelante en el mismo artículo un apartado dedicado a algunas de las normativas legales actualmente vigentes en España). El incumplimiento de estas regulaciones puede resultar en multas y sanciones financieras, lo que puede ser costoso para las empresas.

Ciberseguridad en la cadena de suministro: Las empresas están cada vez más interconectadas, lo que hace que sea difícil protegerse contra los ataques cibernéticos en la cadena de suministro. En concreto, Accenture cifra en un 40% el número de brechas de seguridad que las empresas sufren por esta vía[6]. Las empresas deben asegurarse de que sus proveedores y socios comerciales cumplan con los mismos estándares de seguridad que ellos para minimizar los riesgos.

III
¿Qué se puede hacer en este contexto? Técnicas y herramientas que se utilizan para prevenir y mitigar los ataques informáticos en el mundo empresarial

Las organizaciones, antes de nada, deben realizar una adecuada gestión de activos, para enfocarse en identificar y gestionar cualquier activo que esté relacionado con la información, personas, dispositivos, sistemas e infraestructura de la organización, para garantizar que se manejen adecuadamente de acuerdo con la criticidad de la función de negocio que se proporciona, así como con los objetivos y estrategias de riesgo de la organización. Y, acto seguido, es necesario que la organización tenga una clara identificación y definición de su misión, objetivos, procesos y actores relacionados para poder establecer una estrategia de ciberseguridad adecuada. Esta estrategia deberá definir los roles y responsabilidades en cuanto a la ciberseguridad, y se tomarán decisiones sobre la gestión de los riesgos tecnológicos de cada elemento que forme parte del ecosistema de la organización, considerando:

6 Fuente: Annual State of Cyber Resilience, ACCENTURE.

El modelo de gobernanza de IT en la empresa

El modelo de evaluación / valoración de riesgos

La metodología de gestión y tratamiento de riesgos

En función de dicha metodología y tratamiento de riesgos, todos los identificados que superen el apetito de riesgo de una organización deben ser abordados adecuadamente, de alguna de las siguientes formas[7]:

Eliminando el riesgo: sustituyendo el recurso afectado por la amenaza o eliminado/modificando la actividad que lo generaba.

Reduciendo/mitigando el riesgo: implementando medidas apropiadas para que el nivel de riesgo se encuentre por debajo del apetito de riesgo establecido (disminuyendo la probabilidad, aplicando controles de seguridad compensatorios, etc.).

Transfiriendo el riesgo: si la organización no puede gestionar el riesgo, contratando a un tercero para que se encargue de controlarlo y mantenerlo por debajo del límite establecido.

Aceptando el riesgo: cuando el riesgo está por debajo del límite, o cuando los costes relacionados con su tratamiento son tan altos que la organización opta por asumirlos. En ciertos casos, la entidad puede determinar que los beneficios asociados superan el riesgo.

Para lograr una gestión de riesgos exitosa, es crucial establecer claramente los objetivos y asegurar el compromiso de toda la organización, pudiéndose seguir al efecto algunas de las siguientes tendencias actuales en ciberseguridad empresarial:

7 Fuente: Gestión de Riesgos, Departamento de Desarrollo Internacional, Gobierno de Reino Unido.

Mayor enfoque en la prevención

El mundo empresarial está tomando medidas proactivas para evitar ataques cibernéticos, en lugar de simplemente responder a ellos después de que hayan ocurrido. Esto incluye la implementación de medidas de seguridad que hagan que sea más difícil, o mejor dicho menos probable, que un ataque informático se materialice.

Incrementar las capacidades de respuesta

Existen muchas empresas que dan por descontado que serán atacadas por un ataque de ciberseguridad, por lo que apuestan firmemente por ser capaces de detectar dichos ataques lo antes posible para, de esta manera, reaccionar rápidamente de forma reactiva y mitigar así el impacto de las amenazas.

... y, en definitiva, realizar una mayor inversión en tecnología de ciberseguridad...

Las empresas están invirtiendo cada vez más en tecnología de ciberseguridad, como software de seguridad, hardware de seguridad y servicios de seguridad administrados. También están invirtiendo en personal capacitado para manejar esta tecnología y garantizar la seguridad de los sistemas y datos de la empresa. A nivel tecnológico, los siguientes componentes[8] - sin ser una lista exhaustiva - podrían considerarse clave en la lucha contra los atacantes cibernéticos:

Cortafuegos (también llamado firewall): Un cortafuegos es un software o hardware que se utiliza para filtrar el tráfico de red y bloquear el acceso no autorizado a un sistema o red. Los cortafuegos pueden ser configurados para permitir o bloquear el tráfico de entrada y salida y para permitir o denegar el acceso a ciertos sitios web.

Antivirus: Un antivirus es un software que se utiliza para detectar y eliminar virus, malware y otras amenazas informáticas. Los antivirus pueden ser instalados en computadoras individuales o en toda la red.

8 Fuente: Protegiendo lo que importa: Las principales medidas de seguridad para proteger tu organización, CISO Advisory Board, Jose María Labernia.

Actualizaciones de seguridad y configuración segura: Las actualizaciones de seguridad son parches o actualizaciones de software que se lanzan para corregir vulnerabilidades conocidas en el software. Es importante mantener el software actualizado y configurado de forma robusta para protegerse contra las últimas amenazas.

Autenticación de dos factores: La autenticación de dos factores es un método de autenticación que utiliza dos elementos diferentes para verificar la identidad de un usuario. Por ejemplo, se puede requerir una contraseña y un código de verificación enviado por mensaje de texto para acceder a una cuenta.

Encriptación: La encriptación es un método de protección de datos que convierte los datos en un formato ilegible para cualquier persona que no tenga la clave de encriptación. La encriptación se utiliza para proteger datos confidenciales, como números de tarjeta de crédito y contraseñas.

Pruebas de penetración: Las pruebas de penetración son pruebas de seguridad que se realizan para evaluar la resistencia de un sistema o red a los ataques informáticos. Los expertos en seguridad informática realizan pruebas de penetración para identificar posibles vulnerabilidades y recomendar medidas de seguridad adicionales.

IV

... y si fracasamos en los procesos, personas y tecnologías a aplicar, siempre queda la ley y la monitorización constante como garante cibernético:

La Ley es el principio superior que determina el orden; es como dijo San Agustín "una cierta regla y medida de los actos que induce al hombre a obrar o lo retrae de actuar"

"La Ley, en su magnanimidad, no solo prohíbe cualquier acción que pueda ser dañina para la sociedad, sino que también procura que las per-

sonas no hagan nada que pueda ser perjudicial para ellas mismas". En esta cita atribuída a Miguel de Cervantes, se destaca la importancia de las leyes en la protección de la sociedad y los individuos. Sugeriría Cervantes que la ley no solo se preocupa por proteger a la sociedad de acciones perjudiciales, sino también por proteger a los individuos de hacerse daño a sí mismos. La ley es necesaria para establecer límites claros y equitativos para la conducta humana y para garantizar que la sociedad funcione de manera justa y equitativa.

De la misma manera ocurre en el mundo empresarial, donde el imperio de la Ley debe regir, ayudando (i) a las autoridades encargadas de hacer cumplir la ley a investigar los ataques informáticos y enjuiciar a los autores (incluso incluyendo la identificación y el arresto de los delincuentes cibernéticos, la recuperación de los datos robados y la presentación de cargos criminales), ii) a imponer sanciones y multas a las empresas y organizaciones que no cumplan con los requisitos de ciberseguridad, ayudando a disuadir a las empresas de no tomar medidas adecuadas de ciberseguridad y protegerse contra los riesgos informáticos, iii) a establecer normas y requisitos para la ciberseguridad, como la necesidad de proteger los datos personales de los clientes y empleados y la obligación de notificar las violaciones de seguridad, y por último, iv) a proporcionar un marco legal para la cooperación entre las empresas y las autoridades encargadas de hacer cumplir la ley en la lucha contra los ataques informáticos, incluyendo la compartición de información y la colaboración en la investigación y enjuiciamiento de los delincuentes cibernéticos.

Cabe destacar que la evolución de hechos conocidos de cibercriminalidad en España no ha parado de aumentar en la última década, disparándose a niveles récord en el último lustro. En concreto, el total de delitos cibernéticos denunciados o conocidos en el año 2017 fueron más de 117.000. Cinco años más tarde, el mismo indicador arroja más de 305.000 delitos, de los cuales únicamente 46.000 fueron esclarecidos y 13.801 dieron lugar a investigaciones de mayor calado y detenciones. Los delitos, en su mayor porcentaje, son debidos a fraudes informáticos, pero también tienen una relevancia significativa otros como los relativos a las amenazas y coacciones, los delitos contra el honor,

falsificaciones informáticas o incluso delitos contra la propiedad intelectual o industrial[9].

Ante esta situación, las organizaciones deben conocer la normativa legal más relevante - que no es poca - que afecta a la ciberseguridad y servicios digitales de su región, y apostar por su conocimiento y cumplimiento para reducir el impacto de los riesgos de ciberseguridad en el contexto actual. Algunas de las normativas más relevantes a nivel internacional y estatal serían las siguientes[10]:

(UE) 2016/679 sobre protección de datos personales (GDPR conocida comúnmente en Europa): El Reglamento General de Protección de Datos (GDPR) es una normativa de la UE que establece las normas para la protección de datos personales. La GDPR es aplicable a cualquier organización que procese datos personales de ciudadanos de la UE, independientemente de dónde se encuentre la organización. La norma GDPR establece requisitos para el tratamiento de datos personales, incluyendo el consentimiento del titular de los datos, el derecho a la eliminación de datos y la obligación de notificar a los titulares de los datos en caso de violaciones de seguridad.

Directiva NIS (UE) sobre seguridad de las redes y sistemas de información 2016/1148: La Directiva sobre Seguridad de las Redes y Sistemas de Información (NIS) es una normativa de la UE que establece requisitos para la seguridad cibernética en los sectores críticos, como la energía, el transporte, la salud y los servicios financieros. La directiva NIS establece requisitos de seguridad para las empresas y organizaciones en estos sectores, incluyendo la obligación de informar sobre incidentes de seguridad, la realización de evaluaciones de riesgos y la implementación de medidas de seguridad adecuadas.

9 Fuente: Informe sobre la cibercriminalidad en España año 2021, Secretaría de Estado de Seguridad, Ministerio del Interior, Gobierno de España.

10 Fuente: Instituto Nacional de Ciberseguridad (INCIBE), Ministerio de Asuntos Económicos y Transformación Digital, Gobierno de España.

Directiva UE 2019/790: sobre derechos de autor y derechos afines en el mercado único digital.

Directiva Servicios de pago (UE) 2015/2366 y Reglamento PSD2 (UE) 2015/751: desarrollada para mejorar la seguridad y protección de los consumidores en relación con los servicios de pago, así como fomentar la innovación y competencia en el mercado de pagos electrónicos.

R.D-ley 12/2018 de seguridad de las redes y sistemas de información: establece un marco regulatorio para proteger la seguridad de las redes y sistemas de información en España, con especial énfasis en la protección de infraestructuras críticas y la prevención y respuesta a incidentes de seguridad.

Ley 9/2014 Telecomunicaciones (LGT): establece el marco regulatorio para el sector de las telecomunicaciones en España, con el objetivo de fomentar la competencia, garantizar el acceso universal a los servicios de telecomunicaciones y proteger los derechos de los usuarios.

Ley 8/2011 Medidas protección infraestructuras críticas (IICC) R.D. 704/2011 Reglamento Protección infraestructuras críticas: establecen un marco regulatorio para la protección de las infraestructuras críticas en España, con el objetivo de garantizar su seguridad y funcionamiento en caso de crisis.

R.D. 3/2010 Esquema Nacional de Seguridad (ENS): normativa que establece los requisitos y medidas de seguridad que deben cumplir los sistemas y tecnologías de la información utilizados por las Administraciones Públicas en España, con el objetivo de proteger la información y garantizar su seguridad.

Ley 59/2003 Firma electrónica (LFE): establece un marco jurídico para la utilización de la firma electrónica en España, reconociendo su validez jurídica y estableciendo medidas para garantizar su autenticidad e integri-

dad, así como la identificación del firmante. La LFE tiene como objetivo fomentar la utilización de las nuevas tecnologías en las relaciones jurídicas y comerciales en España.

Ley 34/2002: Servicios Sociedad Información y comercio electrónico (LSSICE): tiene como objetivo garantizar la transparencia y la seguridad en el comercio electrónico y en los servicios de la sociedad de la información en España.

Norma ISO 27001: Sin ser una ley a cumplir sino un marco de referencia de los profesionales de seguridad, la norma ISO 27001 establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Esta norma proporciona un marco para establecer políticas y procedimientos de seguridad de la información en una organización y asegurarse de que se cumplan los requisitos legales y regulatorios.

Conocer y monitorizar el cumplimiento de las leyes anteriores es fundamental para garantizar el cumplimiento legal, proteger los datos personales y sensibles de los usuarios, mejorar la competitividad y prevenir riesgos y amenazas de la seguridad en internet.

Dado lo extenso de las normas en vigor, las evaluaciones de seguridad son cruciales para el avance en la madurez de los protocolos de protección de una organización. Estas evaluaciones permiten reconocer las vulnerabilidades en cuanto a seguridad y proponer soluciones apropiadas para reducir riesgos, y las organizaciones deben realizarlas para poder entender los riesgos que están asumiendo y poder hacer una gestión efectiva de los mismos.

Generalmente, estas evaluaciones son externalizadas, y se contratan empresas especializadas en análisis de seguridad para asegurar la objetividad de los resultados. Un examen de seguridad incluye análisis de vulnerabilidades en direcciones IP y sitios web de la infraestructura externa crítica, así como encuestas o entrevistas a empleados para evaluar las prácticas reales de ciberseguridad.

V
En conclusión a todo lo anterior

La ciberseguridad en las empresas es un tema cada vez más relevante en el mundo empresarial. Con el avance de la tecnología y la digitalización, las amenazas y riesgos en línea se han multiplicado, por lo que es fundamental que las empresas tomen medidas para protegerse y cumplir con las leyes y regulaciones en materia de seguridad.

Como dijo el jurista romano Ulpiano, los principios o las tres máximas del Derecho son: ***"honeste vivere, alterum non laedere, suum cuique tribuere:*** **La justicia es la constante y perpetua voluntad de dar a cada uno lo que le corresponde"**.

En el mundo digital, esta justicia se manifiesta en el **compromiso de las empresas de proteger los datos y la privacidad de sus clientes y usuarios, cumpliendo con las leyes y normativas establecidas**. De esta forma, las empresas no solo protegen su reputación y seguridad, sino que también contribuyen a una sociedad más justa y equitativa en línea.

UNA REVISIÓN BIBLIOMÉTRICA DE LA INVESTIGACIÓN SOBRE CIBERSEGURIDAD Y NEGOCIOS, 2004-2022.

Ana Maria Gil-Lafuente
Académica de Número de la Real Academia de Ciencias Económicas y Financieras

Luciano Barcellos-Paula
CENTRUM Cátolica Graduate Business School

La ciberseguridad resulta un riesgo crítico para las empresas por el incremento de ciberataques en diversas partes del mundo, lo que aumenta la incertidumbre en el proceso de su gestión y, a su vez, pone en peligro la sostenibilidad de sus negocios. Los objetivos de esta investigación son: (i) identificar la base de conocimientos sobre ciberseguridad y negocios y su estructura intelectual; y (ii) conocer el avance científico y ampliar la discusión en esta disciplina. Como metodología, los autores realizan una revisión bibliométrica a través de un mapeo científico y un análisis del rendimiento. La investigación utiliza la base de datos de la Web of Science, y el software Bibliometrix para analizar 310 artículos en nueve indicadores bibliométricos en un periodo de 19 años. Los principales resultados revelan una tendencia al alza de las publicaciones con un crecimiento anual del 27.56% y muestran a Estados Unidos como el país con más producción científica seguido de Reino Unido y China. Otros hallazgos indican como temas de tendencia enterprises, features, y models. La principal contribución radica en reducir las brechas de conocimiento identificadas para minimizar los riesgos cibernéticos en la gestión empresarial. El estudio presenta futuras líneas de investigación sobre ciberseguridad.

Palabras clave: ciberseguridad, negocios, incertidumbre, mapeo científico, riesgos, sostenibilidad, bibliometrix.

1. Introducción

La ciberseguridad es un riesgo clave para cualquier empresa debido al incremento exponencial de las ocurrencias (Bresniker et al., 2019) y la sofisticación de los ataques (Abeshu & Chilamkurti, 2018). En esta misma línea los investigadores advierten del surgimiento de grupos organizados, preparados y persistentes que atacan a las empresas para obtener beneficios financieros (Ahmad et al., 2021). Durante la pandemia provocado por la COVID-19, tanto la ciberdelincuencia como el fraude aumentaron por encima de los niveles previstos (Kemp et al., 2021). Estos ciberataques provocan consecuencias negativas para las organizaciones como la pérdida de productividad, falta de confianza de los clientes y sanciones legales (Ahmad et al., 2021). Además, el riesgo cibernético puede afectar la marca, la reputación, la competitividad, el valor financiero y la sostenibilidad de los negocios (Ngoc Thach et al., 2021). Por estas razones la ciberseguridad es una preocupación creciente en la mayoría de las organizaciones (Kappelman et al., 2022).

La industria 4.0, las nuevas tecnologías e internet permitieron a las empresas e industrias de beneficiarse de las plataformas en la nube y de la infraestructura como servicio (IaaS) que proporciona capacidades esenciales de cómputo, almacenamiento y redes (Bhamare et al., 2020). Los mismos autores indicaron que la computación en nube para los Sistemas de Control Industrial (SCI) presentes en los sectores industriales y las infraestructuras críticas muestran ventajas como la escalabilidad, la rentabilidad y la flexibilidad (Bhamare et al., 2020). Sin embargo, al pasar a la nube los SCI pueden quedar expuestos a nuevas amenazas y vulnerabilidades (Bhamare et al., 2020). Otros investigadores asociaron los posibles problemas de seguridad debido al uso de sistemas y redes abiertos para la comunicación y el control (Kosmowski et al., 2022). Para hacer frente a estos inconvenientes y lograr un nivel adecuado de ciberseguridad, las soluciones tecnológicas, como los programas antivirus, firewalls, sistemas de detección de intrusos, redes privadas virtuales, sistemas de control de acceso y filtros de contenido, necesitan de enfoques más avanzados y colaborativos (Rashid et al., 2021).

La creciente disponibilidad de Internet modificó las actividades laborales y de ocio al facilitar el acceso a la información y la comunicación. No obstante, los delincuentes dedican más tiempo a los delitos en línea como el fraude cibernético (Kemp et al., 2021). Asimismo, el uso de internet en diversos sectores dejó a las empresas más expuestas a los riesgos cibernéticos (Rashid et al., 2021). Por ejemplo, el número de casos de ciberdelincuencia aumenta constantemente en la banca electrónica en línea (Ngoc Thach et al., 2021). Las organizaciones de atención médica son vulnerables a las ciber amenazas (Jalali et al., 2019) ya que los ciberataques pueden comprometer la integridad de los datos y afectar la funcionalidad de los dispositivos médicos (Jalali et al., 2019). En el sector industrial, los riesgos surgen cuando las empresas adoptan las tecnologías de la Industria 4.0 (Kosmowski et al., 2022), y la falta de seguridad adecuada en las nuevas plataformas multi-nube puede causar altos costes asociados a las brechas de seguridad en las plataformas industriales en tiempo real (Bhamare et al., 2020). Las infraestructuras críticas como las centrales nucleares y térmicas, las instalaciones de tratamiento de aguas, las industrias pesadas y los sistemas de distribución pueden quedar expuestos a nuevas amenazas y vulnerabilidades (Bhamare et al., 2020). Los problemas derivados de los ciberataques también pueden perturbar al sector energético como las empresas de energía industrial, las centrales eléctricas y las centrales de energía renovable distribuida (Kosmowski et al., 2022).

Por otra parte, la falta de inversión en ciberseguridad impactan en el aumento de los riesgos, los costes económicos de los incidentes, las pérdidas sociales y la reducción de los niveles de seguridad individual y nacional (Rashid et al., 2021). Por estas razones, las organizaciones necesitan invertir en ciberseguridad para adaptarse con rapidez y eficacia y mejorar la calidad de gestión de la tecnología (Ngoc Thach et al., 2021). En esta dirección los niveles de gasto en tecnología de información están volviendo desde los máximos inducidos por la Covid en 2020 (Kappelman et al., 2022). Los gestores también deben entender cómo las organizaciones pueden protegerse frente a ciberataques sofisticados y persistentes, siendo este un reto importante tanto para la investigación como para la práctica (Ahmad et al., 2021). Además, el sector

industrial necesita comprender los riesgos que entrañan los posibles ciberataques al adoptar las tecnologías de la Industria 4.0 (Kosmowski et al., 2022).

La ciberseguridad también está vinculada a los Objetivos de Desarrollo Sostenible (ODS) principalmente al ODS 8 - Trabajo decente y crecimiento económico - y al ODS 9 - Industria, innovación e infraestructura - pues los problemas provocados por los ciberataques afectan directamente al trabajo, la industria y la economía. En 2015, las Naciones Unidas (United Nations, 2018) lanzó los ODS con la finalidad de orientar a los países, las empresas y la sociedad hacia un desarrollo sostenible a través de la agenda 2030. Con todo la revisión de la literatura identificó pocas investigaciones científicas que relacionan ciberseguridad y negocios, con los ODS. El uso de los ODS como un marco general permite integrar diferentes herramientas, políticas y estrategias (Croese et al., 2020). En esta dirección, las estrategias de inversión de ciberseguridad, tecnologías disruptivas y robótica pueden promover los ODS sin sacrificar los rendimientos de las empresas (Naffa & Fain, 2020). Otros autores resaltaron la importancia de ciberseguridad para apoyar las plataformas de cursos en línea y contribuir al ODS 4 - Educación de calidad - (Robles-Gomez et al., 2021). Además, algunos investigadores propusieron un modelo de negocio que permite la transición orientada a lo digital hacia la sostenibilidad fomentando un mayor desarrollo de la Industria 4.0 (ciberseguridad, integración de sistemas, computación en la nube, big data e Internet de las cosas) y al mismo tiempo contribuye a los ODS 8 y 9, y al ODS 12 – Producción y consumo responsables - (Kluczek et al., 2023).

En resumen, la ciberseguridad resulta un riesgo crítico para las empresas por el incremento de ciberataques en diversas partes del mundo (Bresniker et al., 2019) lo que aumenta la incertidumbre en el proceso de su gestión y, a su vez, pone en peligro la sostenibilidad de sus negocios (Kosmowski et al., 2022). La revisión de la literatura identificó tres brechas de conocimiento sobre ciberseguridad y negocios. La primera brecha se refiere a la conciencia de la situación como atributo crítico de la respuesta organizativa a incidentes (Ahmad et al., 2021). Las empresas deben comprender a qué riesgos ciber-

néticos están expuestos (Kosmowski et al., 2022). La segunda brecha radica en la existencia de pocos estudios que relacionan ciberseguridad y negocios con los ODS. La tercera brecha está en que la revisión de literatura identificó solamente una publicación de análisis bibliométrico sobre ciberseguridad que se dedica al sector salud (Jalali et al., 2019).

En este contexto, la ciencia ejerce un papel significativo (Bresniker et al., 2019) para encontrar soluciones a los problemas identificados, reducir las brechas de conocimiento y generar un impacto positivo a la sociedad al contribuir al logro de los ODS. Dada la creciente importancia de los temas mencionados, es necesario profundizar las investigaciones sobre ciberseguridad y negocios. En este sentido, las bases de datos científicas revelan un incremento de publicaciones sobre ciberseguridad y negocios en los últimos años. Sin embargo, este aumento de artículos científicos publicados se desarrolla de manera fragmentada y con carencias al integrar estas informaciones (Aria & Cuccurullo, 2017), lo que dificulta los análisis de investigadores, gestores y responsables políticos. Por estas razones, el mapeo científico es una actividad esencial para los estudiosos de todas las disciplinas científicas (Aria & Cuccurullo, 2017), ya que permite determinar la estructura y conocer el frente de investigación de los ámbitos científicos.

A pesar de los avances la revisión de la literatura identificó brechas de conocimiento sobre ciberseguridad y negocios. Por lo tanto, la principal motivación del estudio radica en reducir estas brechas, y avanzar en la frontera del conocimiento al realizar una revisión bibliométrica en esta disciplina. En función de los argumentos y problemas identificados, los autores buscarán responder las siguientes preguntas de investigación:

P1. ¿Cuál es la base de conocimientos sobre ciberseguridad y negocios, y su estructura intelectual?

P2. ¿Cuál es el frente de investigación sobre ciberseguridad y negocios?

P3. ¿Cómo ciberseguridad en los negocios contribuye a los ODS?

Como metodología, los autores realizan una revisión bibliométrica a través de un mapeo científico y un análisis del rendimiento (Cobo et al., 2011). La investigación utiliza la base de datos de la Web of Science (WoS) y el software Bibliometrix (Aria & Cuccurullo, 2017) para analizar 310 artículos en nueve indicadores bibliométricos en un periodo de 19 años.

Los principales resultados revelan una tendencia al alza de las publicaciones con un crecimiento anual del 27.56% y muestran a Estados Unidos (EE. UU.) como el país con más producción científica, seguido de Reino Unido, y China. Otros hallazgos indican como temas de tendencias enterprises, features, y models. Como principales contribuciones teóricas, el estudio avanza la frontera del conocimiento y reduce las brechas identificadas para minimizar los riesgos cibernéticos. A nivel práctico, las principales contribuciones están en ampliar la discusión sobre ciberseguridad y negocios, y mejorar los análisis de gestores y responsables políticos para generar impacto positivo en la sociedad. Una limitación en la investigación sería considerar solamente artículos en idioma inglés. El estudio presenta futuras líneas de investigación sobre ciberseguridad y negocios como el desarrollo de modelos y algoritmos para reducir la incertidumbre.

Los objetivos de esta investigación son: (i) identificar la base de conocimientos sobre ciberseguridad y negocios, y su estructura intelectual, y (ii) conocer el avance científico y ampliar la discusión en esta disciplina. Esta investigación es novedosa al proponer una revisión bibliométrica sobre ciberseguridad y negocios. Este capítulo está organizado en cinco partes. La sección 2 explica la metodología. La sección 3 presenta los resultados. La sección 4 detalla las discusiones. La sección 5 indica las conclusiones del estudio seguidas de las referencias utilizadas.

2. Metodología

Esta sección presenta la metodología utilizada en esta investigación. La revisión bibliométrica sigue un enfoque combinado (Noyons et al., 1999)

con el mapeo científico y el análisis del rendimiento. Según otros autores (Cobo et al., 2011) el mapeo científico muestra la estructura y los aspectos dinámicos de la investigación científica. Por otro lado, el análisis de rendimiento muestra la evaluación de los grupos de científicos y el impacto de su actividad en la base de datos bibliográfica (Cobo et al., 2011). Los autores utilizan un flujo de trabajo estructurado en cinco etapas para realizar la revisión bibliométrica (Zupic & Čater, 2015). La figura 1 presenta el flujo de trabajo.

Figura 1. Flujo de trabajo

La primera etapa consiste en el diseño del estudio, que incluye las preguntas de investigación, el periodo de análisis y los indicadores bibliométricos. Los autores fijan el periodo de 19 años, comprendido entre 2004 y 2022 para realizar el estudio, ya que no hay artículos publicados antes de este periodo con la combinación de palabras-clave “cybersecurity” y “business”. En seguida los autores eligen nueve indicadores: producción científica anual, producción por países, análisis de palabras-clave, análisis de publicaciones, análisis de autores, análisis de instituciones, análisis de revistas, colaboración entre países, y análisis temático.

La segunda etapa destina a la recopilación de los datos y los autores seleccionan la base de datos de la Web of Science (WoS). Para algunos investigadores (Aria & Cuccurullo, 2017), la WoS es preferible a otras bases de datos en cuanto a la calidad de los datos. Por ejemplo, en Scopus los elementos de referencia mencionados no están normalizados y deben combinarse. Por otro lado, en Dimensions el algoritmo que clasifica las áreas de búsqueda no es eficiente (Aria & Cuccurullo, 2017). Los autores utilizan las palabras-clave "cybersecurity" y "business", y consideran sólo artículos en el idioma inglés. Los datos fueron extraídos de la WoS del 29 al 30 de abril de 2023 en formato de texto plano. Este formato es preferible a otros, ya que el formato BibTeX de Scopus y el formato CSV de Dimensions no permiten exportar algunos metadatos (Aria & Cuccurullo, 2017). Tabla 1 presenta un resumen de la recogida de los datos. Los principales resultados revelan 310 artículos; una tasa de 27.87% de crecimiento anual; 1,144 palabras-clave del autor; 1,054 autores; y el 31.39% de coautoría internacional.

La tercera etapa dedica al análisis de datos, y los autores emplean el software Bibliometrix (Aria & Cuccurullo, 2017) a través de la aplicación web Biblioshiny para analizar los artículos. Los autores prefirieron esta herramienta informática, ya que otros instrumentos especializados suelen realizar sólo algunos pasos del análisis de mapeo científico (Aria & Cuccurullo, 2017). Esta herramienta es de código abierto y permite realizar un análisis completo del mapeo de la literatura científica. Además, es una herramienta amigable para no programadores facilitando la aplicación de este tipo de estudio por otros académicos en su campo de investigación. Tras finalizar el cargamento de la base de datos, los autores realizaron una prueba de calidad de los datos en Bibliometrix y los resultados mostraron que los metadatos no presentan problemas críticos y la mayoría de los indicadores se encuentran en los niveles excelente y bueno. De esta manera los autores proceden con los análisis de datos.

Tabla 1. Resultados de la recopilación de los datos

Descripción	Resultados
PRINCIPAL INFORMACIÓN SOBRE LOS DATOS	
Duración	2004:2022
Fuentes (revistas, libros, etc.)	195
Documentos	310
Tasa de crecimiento anual %	27.56
Edad media del documento	2.87
Citas medias por documento	10.86
Referencias	15,334
CONTENIDO DEL DOCUMENTO	
Palabras clave Plus (ID)	439
Palabras clave del autor (DE)	1,144
AUTORES	
Autores	1,054
Autores de documentos individuales	44
COLABORACIÓN DE AUTORES	
Documentos individuales	48
Coautores por doc	3.61
Coautorías internacionales %	31.29
TIPOS DE DOCUMENTOS	
artículo	310

Nota: DE (distribución de frecuencias de las palabras clave de los autores); ID (distribución de frecuencias de las palabras clave asociadas al manuscrito por la base de datos ISI Web of Knowledge de Thomson Reuters). Fuente: WoS (2023) y Bibliometrix (2023).

La cuarta etapa contempla la visualización de los datos, y los autores utilizarán métodos de visualización como análisis temporal, tablas informativas, análisis de agrupamiento, redes temáticas, mapas de proximidad, y análisis geoespacial (Aria & Cuccurullo, 2017). Finalmente, la quinta etapa consiste en la interpretación de datos. La siguiente sección presenta los resultados de la revisión bibliométrica.

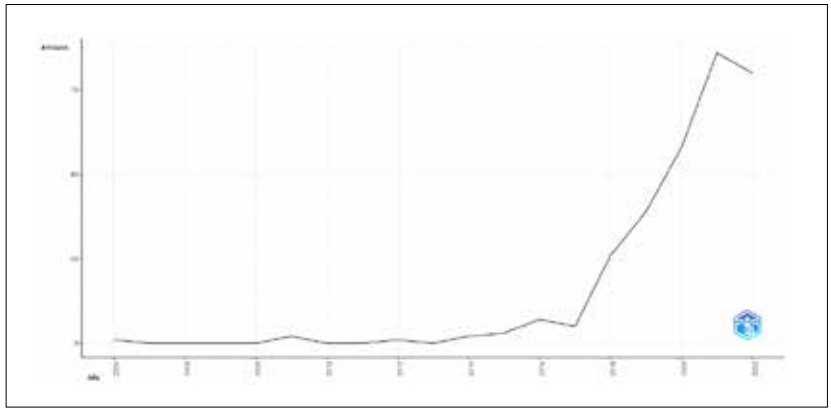
3. Resultados de la revisión bibliométrica

Esta sección muestra los resultados de la revisión bibliométrica a través de figuras y tablas con los respectivos análisis y en el siguiente orden: producción científica anual, producción por países, análisis de palabras-clave, análisis de publicaciones, análisis de autores, análisis por instituciones, análisis de revistas, colaboración entre países, y análisis temático.

3.1 Producción científica anual

Esta subsección presenta el número de artículos publicados en el periodo de 2004 a 2022. La producción científica muestra los resultados de la investigación entre académicos, que buscan avanzar la frontera del conocimiento y dar respuestas a las necesidades de la sociedad (BarcellosŒPaula et al., 2022). Este indicador permite analizar la evolución en el tiempo del tema "cybersecurity" y "business". La figura 2 revela un crecimiento expresivo en la producción científica a partir del 2018, con 28 artículos en este año, y alcanzando 87 artículos en 2021, y 80 artículos en 2022.

Figura 2. Producción científica anual



Fuente: WoS (2023) y Bibliometrix (2023).

3.2 Producción por países

Esta subsección muestra el número de publicaciones de artículos científicos por países. La tabla 2 indica que los EE.UU. lideran este ranking con 223 publicaciones, seguidos por Reino Unido en la segunda posición con 69 publicaciones, y por China en la tercera posición con 48 publicaciones. España se encuentra en la sexta posición con 29 artículos publicados y Ucrania en la décima posición con 22 publicaciones.

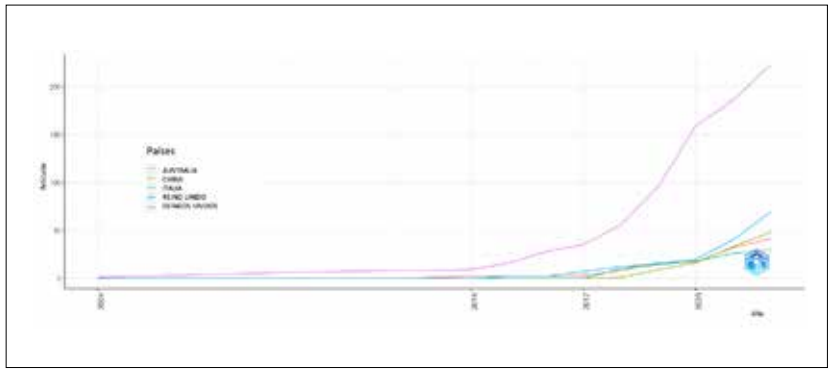
Tabla 2. Producción por países

Países	**N.º de publicaciones**
Estados Unidos	223
Reino Unido	69
China	48
Australia	41
Italia	30
España	29
Arabia Saudita	27
Malasia	24
India	23
Ucrania	22

Fuente: WoS (2023) y Bibliometrix (2023).

Figura 3 exhibe un análisis temporal de la producción científica por países, lo que permite visualizar la evolución de publicaciones y comparar el desempeño entre los países. Los resultados indican que a partir del 2017 la producción científica en EE.UU. se incrementó significativamente, lo que amplió la distancia entre los demás países. Además, Reino Unido consolidó la segunda posición en 2022.

Figura 3. Producción por países en el tiempo



Fuente: WoS (2023) y Bibliometrix (2023).

3.3 Análisis de palabras

Esta subsección analiza las palabras relacionadas con ciberseguridad y negocios. La tabla 3 presenta una lista con las 10 palabras-clave de los autores más frecuentes. Este indicador hace un simple conteo de palabras basado en palabras clave de los autores (Aria & Cuccurullo, 2017). En la primera posición está cybersecurity con 134 ocurrencias, seguido por machine learning con 19 ocurrencias, e internet of things con 16 ocurrencias. Los resultados también revelan risk management con 12 ocurrencias en la séptima posición.

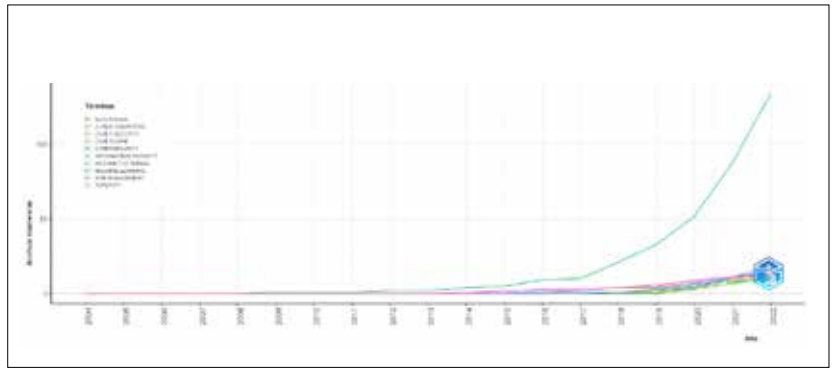
Tabla 3. Palabras más frecuentes

Palabras-clave del autor	Nº de Ocurrencias
cybersecurity	134
machine learning	19
internet of things	16
blockchain	14
security	14
cyber security	13
risk management	12
information security	11
cloud computing	10
cybercrime	9

Fuente: WoS (2023) y Bibliometrix (2023).

La figura 4 exhibe un análisis temporal de las palabras-clave del autor, lo que permite visualizar la evolución en el tiempo entre las 10 palabras-claves más usadas. Los resultados muestran que ciberseguridad ganó relevancia a partir del 2017 y en los últimos años se consolidó como la palabra-clave más utilizada. Los demás términos registraron un crecimiento moderado en los últimos cinco años comparado con *ciberseguridad*.

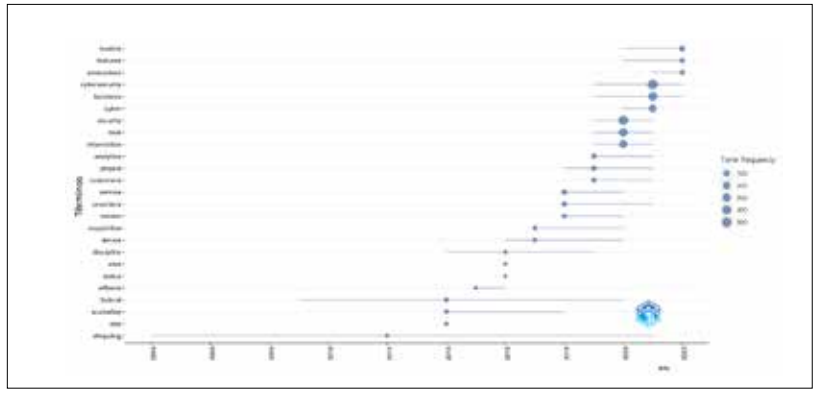
Figura 4. Palabras-clave del autor



Fuente: WoS (2023) y Bibliometrix (2023).

Figura 5 muestra las palabras tendencias en el tiempo. Este indicador permite comprender la evolución del tema *"cybersecurity" y "business"* a lo largo del tiempo. Entre 2004 y 2017, *"cybersecurity" y "business"* se asociaron a diversos temas como *shopping, federal, australian, officers, discipline, device, and acquisition*. Desde 2018, otros contenidos se destacaron como *insider, providers, and service*. En 2019, se introdujeron nuevos temas relacionados con *"cybersecurity" y "business"*, como *customers, project, y analytics*. Solo desde 2020 se produció un aumento significativo de la frecuencia de los términos *information, data, y security*. Por otro lado, en 2021 los investigadores se centraron especialmente en *cyber, business, y cybersecurity*. Finalmente, en 2022 reveló que los temas de tendencias eran *enterprises, features, y models*.

Figura 5. Palabras tendencias en el tiempo



Fuente: WoS (2023) y Bibliometrix (2023).

3.4 Análisis de publicaciones

Esta subsección analiza los documentos más citados, considerando el número de veces que se ha citado cada manuscrito (TC), el número medio anual de veces que se ha citado cada manuscrito (TC por año), y el número de citaciones globales normalizadas (TC normalizada). El TC normalizada se calcula dividiendo el recuento real de elementos citados por el índice de citas esperado para documentos con el mismo año de publicación (Aria & Cuccurullo, 2017). Tabla 4 presenta una lista con los 10 documentos más citados. Los resultados indican la publicación (Babiceanu & Seker, 2016) en primer lugar con 264 citaciones, seguido por el manuscrito (Abeshu & Chilamkurti, 2018) en segundo lugar con 162 citaciones y en tercero lugar, el artículo (Knowles et al., 2015) con 142 citaciones. A continuación, se detalla los principales artículos.

Tabla 4. Documentos más citados

Publicaciones	TC	TC por año	TC normalizada
(Babiceanu & Seker, 2016)	264	33.00	5.22
(Abeshu & Chilamkurti, 2018)	162	27.00	7.13
(Knowles et al., 2015)	142	15.78	2.86
(Al-rimy et al., 2018)	136	22.67	5.99
(Nishant et al., 2020)	117	29.25	8.81
(Leng et al., 2021)	96	32.00	12.75
(Shah, 2020)	95	23.75	7.16
(Ghobakhloo, 2020)	85	21.25	6.40
(Corallo et al., 2020)	78	19.50	5.88
(Li et al., 2019)	73	14.60	5.68

Fuente: WoS (2023) y Bibliometrix (2023).

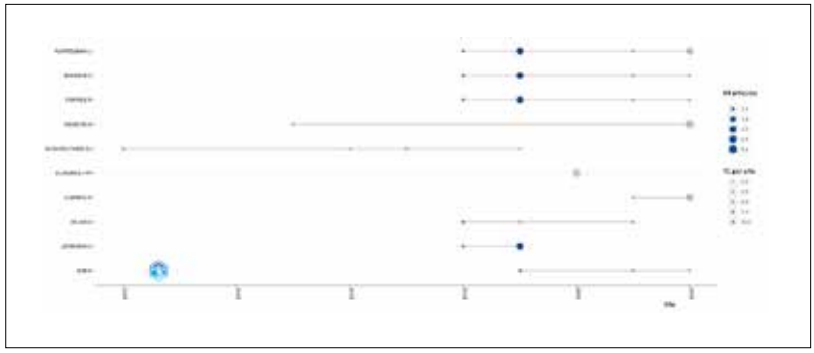
El artículo (Babiceanu & Seker, 2016) ofrece un estado del arte sobre la virtualización y los servicios basados en la nube. El estudio dedica a los sistemas de fabricación y del uso de la analítica de Big Data para la planificación y el control de las operaciones de fabricación. Finalmente, los autores esperan que la fabricación en la nube ofrezca una fabricación empresarial mejorada y ayuda en la toma de decisiones (Babiceanu & Seker, 2016). En el documento (Abeshu & Chilamkurti, 2018) los autores proponen un modelo de aprendizaje distribuido para la detección de ciberataques en la computación. Los resultados muestran que los modelos propuestos son superiores a los superficiales en precisión de detección, tasa de falsas alarmas y escalabilidad (Abeshu & Chilamkurti, 2018). En el manuscrito (Knowles et al., 2015) los investigadores examinan metodologías e investigaciones para medir y gestionar riesgos. El principal hallazgo indicó la escasez de métricas de seguridad específicas para los sistemas de control industrial (Knowles et al., 2015). Finalmente,

otros investigadores (Leng et al., 2021) analizan cómo los sistemas blockchain pueden superar las posibles barreras de ciberseguridad para lograr inteligencia en la Industria 4.0 (Leng et al., 2021).

3.5 Análisis de autores

Esta subsección analiza los autores más relevantes a través de la producción científica en el tiempo. Este indicador calcula y traza la producción de los autores (en términos de número de publicaciones y citaciones totales por año) a lo largo del tiempo. La figura 6 presenta los resultados. Kappelman lidera este ranking con seis publicaciones, seguido por Maurer, y por Torres con cinco artículos cada uno.

Figura 6. Producción de los autores en el tiempo



Fuente: WoS (2023) y Bibliometrix (2023).

La Tabla 5 presenta en detalles la producción de los tres autores, considerando el año de publicación, frecuencia, número de veces que se ha citado cada manuscrito (TC), y el total de citaciones por año (TCpY). Algunos resultados son similares debido a la coautoría entre los tres autores en los principales manuscritos.

Tabla 5. Producción de los tres principales autores

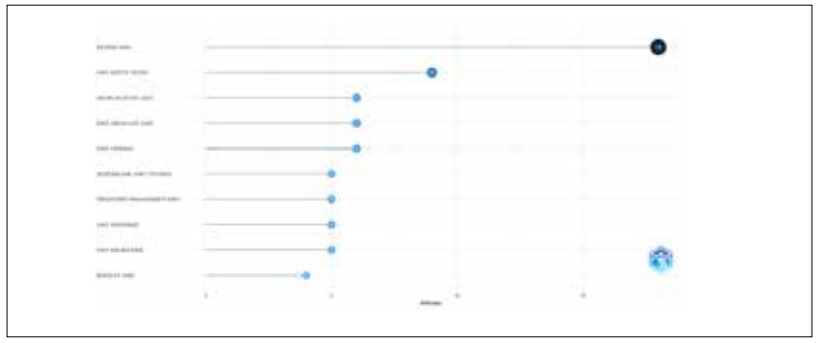
Autores	Año	Frecuencia	TC	TCpY
Kappelman L	2018	1	37	6.167
Kappelman L	2019	2	53	10.6
Kappelman L	2021	1	5	1.667
Kappelman L	2022	2	2	1
Maurer C	2018	1	37	6.167
Maurer C	2019	2	53	10.6
Maurer C	2021	1	5	1.667
Maurer C	2022	1	2	1
Torres R	2018	1	37	6.167
Torres R	2019	2	53	10.6

Fuente: WoS (2023) y Bibliometrix (2023).

3.6 Análisis de instituciones

Esta subsección analiza las instituciones considerando la producción científica, y las redes de colaboración. Figura 7 muestra la Indiana University en primer lugar con 18 publicaciones, la University North Texas en segundo lugar con nueve publicaciones, seguido por Georgia State University, King Abdulaziz University, y University Virginia con seis publicaciones cada una.

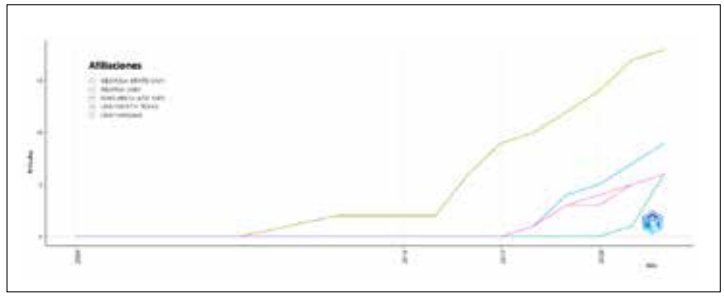
Figura 7. Afiliaciones más relevantes



Fuente: WoS (2023) y Bibliometrix (2023).

La figura 8 presenta un análisis temporal de la producción científica de las afiliaciones. Los resultados revelan que a partir del 2017 Indiana University se consolidó en la primera posición, seguido por la University North Texas. En 2022, se registró una igualdad en número de publicaciones entre Georgia State University, King Abdulaziz University, y University Virginia.

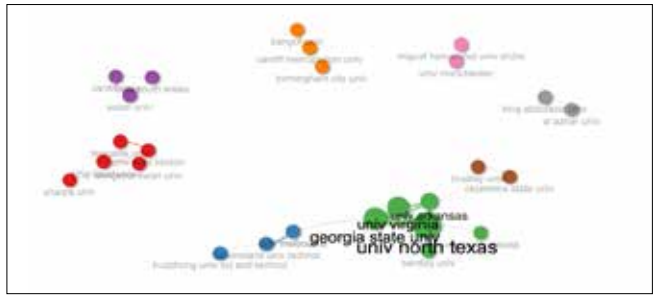
Figura 8. Producción científica de las afiliaciones en el tiempo



Fuente: WoS (2023) y Bibliometrix (2023).

La figura 9 exhibe las redes de colaboración entre las afiliaciones. Cada color representa un grupo diferente. El tamaño de cada nodo representa el número de publicaciones, y el grosor de las líneas es proporcional a su colaboración. Los resultados muestran ocho redes de colaboración, siendo el grupo liderado por Universidad North Texas, color en verde, es el más colaborativo.

Figura 9. Redes de colaboración entre instituciones

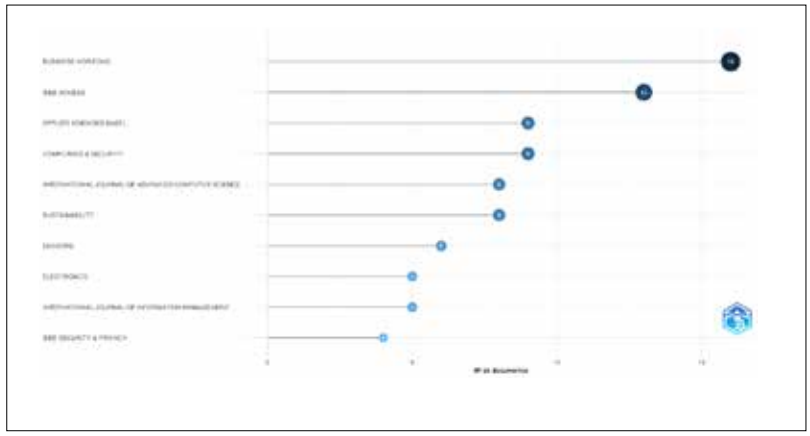


Fuente: WoS (2023) y Bibliometrix (2023).

3.7 Análisis de las revistas

Esta subsección presenta un análisis de las revistas entre 2004 y 2023. Este indicador es relevante, pues las revistas científicas desempeñan un papel esencial en la difusión del conocimiento (BarcellosÕPaula et al., 2022). La figura 10 muestra un análisis de las revistas más influyentes. Los resultados revelan Business Horizons en la primera posición con 16 publicaciones, y en la segunda posición está IEEE Access con 13 publicaciones.

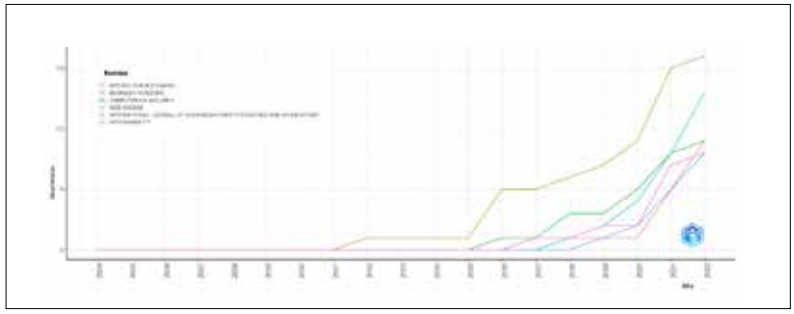
Figura 10. Revistas más relevantes



Fuente: WoS (2023) y Bibliometrix (2023).

La figura11 exhibe un análisis temporal de la producción científica de las revistas. Los resultados permiten visualizar el crecimiento de la revista Business Horizons a partir del 2016, y su consolidación en la primera posición en 2022. Además, con este tipo de análisis es posible notar el crecimiento de todas las revistas representadas en el gráfico, y visualizar el salto de la revista IEEE Access, pasando de la cuarta para la segunda posición en los últimos años.

Figura 11. Producción en las revistas en el tiempo



Fuente: WoS (2023) y Bibliometrix (2023).

3.8 Colaboración entre países

Esta subsección presenta un análisis de la colaboración entre países. Este indicador permite identificar los vínculos de cooperación científica internacional y muestra la difusión del conocimiento a nivel mundial. De este modo, la ciencia puede llegar al mayor número posible de países y contribuir al progreso de la sociedad (BarcellosŐPaula et al., 2022). La figura 12 muestra el mapa de colaboración entre países. Los resultados indican los EE.UU. como el principal responsable por las colaboraciones a nivel mundial, siendo Australia, China, Canadá, India, y Reino Unido los principales destinos colaboradores.

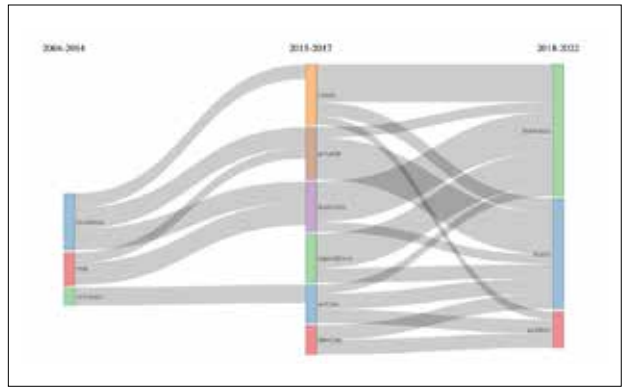
Figura 12. Colaboración entre países

Fuente: WoS (2023) y Bibliometrix (2023).

3.9 Análisis temático

Esta subsección presenta los resultados de los análisis temáticos en tres etapas: análisis de evolución temática, análisis de mapa temático, análisis de red de co-ocurrencias. La primera etapa aborda el análisis de evolución temática basado en el análisis de redes de co-palabras y clustering (Cobo et al., 2011) en los periodos de 2004-2014, 2015-2017, y 2018-2022. Figura 13 muestra que, en el primero periodo, las palabras más incidentes eran business, risk, y enhance. En el segundo periodo (2015-2017), la palabra business se divide en tres grupos cyber, private y business. En el tercero periodo (2018-2022), business agrupa parte de los temas cyber, private, y business, e incluye operations y article. Por otro lado, los resultados revelan el surgimiento de dos nuevos temas study y system entre 2018 y 2022. El tema system agrupa parte de las temáticas cyber, article y device. Por fin, el tema Study agrupa parte de las temáticas cyber, private, business, operations, article y device. Este resultado mostró que a relevancia del tema "study" coincide con la investigación (Bresniker et al., 2019), en que los autores indican que la adopción de la inteligencia artificial y el aprendizaje automático aplicada a la ciberseguridad requiere la asociación de la industria, el mundo académico y la administración pública a escala mundial (Bresniker et al., 2019).

Figura 13. Evolución temática

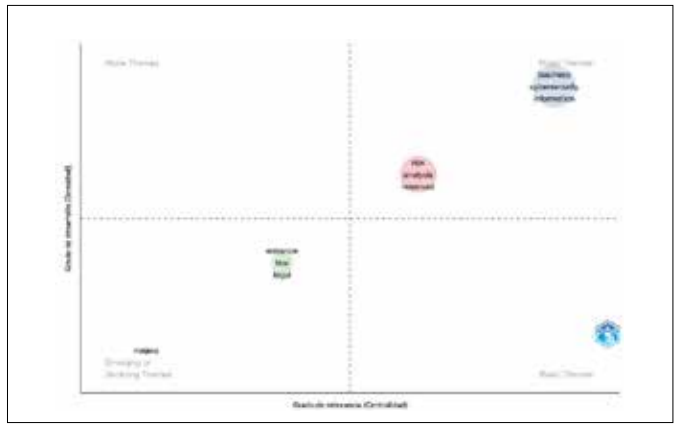


Fuente: WoS (2023) y Bibliometrix (2023).

La segunda etapa presenta el análisis de mapa temático. El análisis de co-palabras extrae grupos de palabras clave. Se consideran temas, cuya densidad y centralidad pueden utilizarse para clasificar los temas y representarlos en un diagrama bidimensional (Aria & Cuccurullo, 2017). El mapa temático es un diagrama intuitivo y sirve para analizar los temas según el cuadrante en el que se sitúen: (1) cuadrante superior derecho: temas motores; (2) cuadrante inferior derecho: temas básicos; (3) cuadrante inferior izquierdo: temas emergentes o en vías de desaparición; (4) cuadrante superior izquierdo: temas muy especializados/nicho (Aria & Cuccurullo, 2017).

La figura 14 presenta el mapa temático entre 2004 y 2014; los resultados indican que el grupo 1 formado por las palabras *business, cybersecurity*, e *information* son temas motores con alto grado de relevancia y de desarrollo. El grupo 2, formado por las palabras *risk, análisis y reserved* también se encuentran en el mismo cuadrante (temas motores) pero con grados de relevancia y de desarrollo inferiores al grupo 1 liderado por *business*. Por otro lado, como temas emergentes se halla el grupo 3 compuesto por las palabras *enhance, law y legal*. En este mismo cuadrante, está la palabra *means* como temas en vías de desaparición.

Figura 14. Mapa temático 2004-2014



Fuente: WoS (2023) y Bibliometrix (2023).

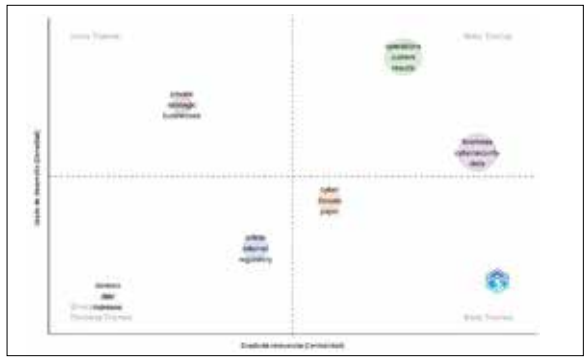
La figura 15 muestra el mapa temático entre 2015 y 2017, y los resultados indican como temas motores dos grupos de palabras. El grupo 1 formado por operations, current y results, y el grupo 2 compuesto por business, cybersecurity, y data. El grupo 1 presenta un grado de desarrollo más alto que el grupo 2. Sin embargo, el grupo 2 presenta un grado de relevancia más elevado que el grupo 1. Por otra parte, como temas nicho se encuentran el grupo 3 formado por las palabras private, strategic y businesses.

Figura 15. Mapa temático 2015-2017

Fuente: WoS (2023) y Bibliometrix (2023).

La figura 16 exhibe el mapa temático entre 2018 y 2022, y los resultados indican que el grupo 1 formado por las palabras business, cybersecurity, y security se encuentra entre los temas motores y básicos, con elevado grado de relevancia y grado medio de desarrollo. Por otro lado, como temas motores y nicho está el grupo 2 compuesto por las palabras study, risk y organizations. En este caso, este grupo de palabras presenta un alto grado de desarrollo, y un grado medio de relevancia.

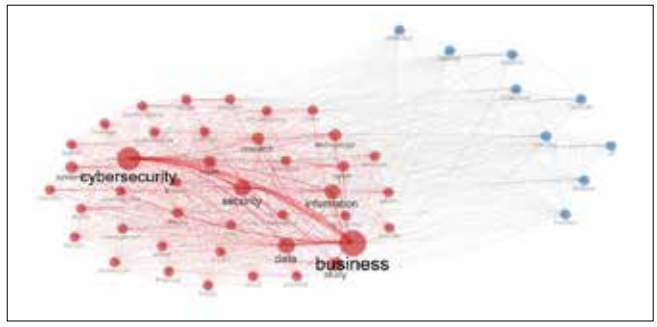
Figura 16. Mapa temático 2018-2022



Fuente: WoS (2023) y Bibliometrix (2023).

Finalmente, la tercera etapa presenta el análisis de red de co-ocurrencias entre palabras. Este indicador hace referencia a una interconexión agrupada de términos, teniendo en cuenta su presencia en los documentos recuperados en la búsqueda en la WoS y permiten visualizar los vínculos entre las palabras e identificar las agrupaciones en red. Cada color representa una agrupación diferente. El tamaño de cada nodo representa la ocurrencia del elemento y el grosor de las líneas es proporcional a su co-ocurrencia. Figura 16 presenta las co-ocurrencias entre las palabras *cybersecurity y business*.

Figura 17. Red de co-ocurrencias



Fuente: WoS (2023) y Bibliometrix (2023).

Los resultados revelan la existencia de dos agrupaciones. La primera, en color roja, muestra que *cybersecurity y business* presentan más ocurrencias, y la segunda, en color azul, revela que *system y proposed* exhiben más ocurrencias. Este resultado confirma la relevancia de las agrupaciones en la red roja lideradas por los términos *business y cybersecurity*.

4. Discusiones

Esta sección presenta las discusiones de los principales resultados de la revisión bibliométrica sobre *"cybersecurity" y "business"*, y las limitaciones del estudio. El estudio reveló un crecimiento expresivo en la producción científica a partir del 2018 hasta el 2022. Este resultado muestra el interés académico por el tema, y la necesidad en responder a una preocupación creciente a la mayoría de las organizaciones (Kappelman et al., 2022). Los resultados también revelaron *risk management* entre las diez palabras con más ocurrencias, lo que coincide con otros investigadores (Kosmowski et al., 2022) al recomendar que las empresas del sector energético deben prepararse a los peligros y amenazas existentes y emergentes, incluidos los ciberataques (Kosmowski et al., 2022). El indicador palabras tendencias en el tiempo revelaron *enterprises, features, y models* como las principales en 2022. Este hallazgo responde a los investigadores (Manuel et al., 2022) que advirtieron sobre la escasez de modelos aplicables y detallados a nivel inferiores para gestionar la ciberseguridad. En este sentido, la investigación propone un modelo con metodología que permita gestionar la ciberseguridad en los niveles inferiores (Manuel et al., 2022).

El análisis del mapa temático entre 2018 y 2022 reveló como temas motores y nicho el grupo de palabras *study, risk y organizations*. En este caso, este grupo de palabras presenta un alto grado de desarrollo y un grado medio de relevancia. Estos resultados responden a los investigadores (Ahmad et al., 2021) que indicaron que para enfrentarse a la amenaza las organizaciones deben desarrollar una conciencia de la situación en sus prácticas de respuesta a incidentes (Ahmad et al., 2021). Asimismo, el mapa temático coincide con hallazgos de otra investigación (Bresniker et al., 2019) que revelan que los

avances en ciberseguridad depende del involucramiento de la industria, academia y administración pública (Bresniker et al., 2019). Por fin, el resultado también confirma sobre que uno de los mayores retos a los que se enfrenta el sector industrial es comprender los riesgos que entrañan los posibles ciberataques (Kosmowski et al., 2022). En resumen, estos resultados reducen la primera brecha de conocimiento sobre necesidad de generar conciencia como respuesta organizativa a incidentes (Ahmad et al., 2021), y comprensión a los riesgos cibernéticos que están expuestos (Kosmowski et al., 2022).

La revisión de la literatura indicó varias causas y efectos relacionadas con ciberseguridad y negocios. Sin embargo, la mayoría de las investigaciones no asocian estos elementos a los impactos que pueden generar al desarrollo sostenible (United Nations, 2018). Por ejemplo, una investigación (Ahmad et al., 2021) mencionó que los ciberataques pueden generar la pérdida de productividad, falta de confianza de los clientes, y sanciones legales. Los autores sugieren incluir que estos problemas afectarían también al ODS 8 (United Nations, 2018). Otra investigación (Ngoc Thach et al., 2021) indicó que el número de casos de ciberdelincuencia aumenta constantemente en la banca electrónica en línea. Este problema afectaría directamente al ODS 8, meta 8.10 - Fortalecer la capacidad de las instituciones financieras nacionales para fomentar y ampliar el acceso a los servicios bancarios, financieros y de seguros para todos (United Nations, 2018). La misma investigación (Ngoc Thach et al., 2021) mostró que el riesgo cibernético puede afectar la marca, la reputación, la competitividad, el valor financiero; y otro estudio (Kosmowski et al., 2022) la sostenibilidad de los negocios. En este caso, no sería posible promover la industrialización sostenible (ODS 9) con los impactos negativos mencionados. Por otra parte, algunos investigadores (Ngoc Thach et al., 2021) sugirieron que las organizaciones necesitan invertir en ciberseguridad para adaptarse con rapidez y eficacia, y mejorar la calidad de gestión de la tecnología. Se recomienda añadir que estas acciones ayudarían también al ODS 9. Otro estudio (Rashid et al., 2021) propone qué soluciones tecnológicas necesitan de enfoques más avanzados y colaborativos. Esta relevante propuesta estaría vinculada al ODS 8 y al ODS 9. Finalmente, otra investigación (Kosmowski et al., 2022) plan-

teó que el sector industrial necesita comprender los riesgos de ciberataques al adoptar las tecnologías. En este caso, los autores recomiendan incluir que esta medida contribuye al ODS 9. En resumen, estos hallazgos reducen la segunda brecha sobre la existencia de pocos estudios que relacionan ciberseguridad y negocios, con los ODS.

De acuerdo con la revisión de la literatura, este estudio es novedoso al realizar una revisión bibliométrica sobre ciberseguridad y negocios, lo que reduce la tercera brecha de conocimiento identificada. Los resultados de los indicadores (producción científica anual, análisis de palabras-clave, análisis de publicaciones, análisis de autores, y análisis temático) responden a la P1 al presentar la base de conocimientos sobre ciberseguridad y negocios, y su estructura intelectual. Por otra parte, los resultados de los indicadores (producción por países, análisis por instituciones, análisis de revistas, y colaboración entre países) responden a la P2 al mostrar el frente de investigación sobre ciberseguridad y negocios. La presentación de causas y efectos relacionadas con ciberseguridad y negocios responden a la P3 al vincular a los ODS 8 y ODS 9. Como limitaciones la investigación consideró solamente artículos en el idioma inglés, y no se consideró el año 2023 por estar incompleto. Artículos en otros idiomas y publicaciones como libros, capítulo de libros y anales de congresos pueden ser usados en futuros estudios.

5. Conclusiones

La investigación identificó la base de conocimientos sobre ciberseguridad y negocios, y su estructura intelectual, y permitió conocer el avance científico en esta disciplina. Los autores utilizaron la base de datos de la WoS y el software *Bibliometrix* para analizar 310 artículos en nueve indicadores bibliométricos en un periodo de 19 años. La revisión de literatura identificó brechas de conocimiento, y amplió la discusión sobre ciberseguridad y negocios.

Los principales resultados revelaron una tendencia al alza de las publicaciones con un crecimiento anual del 27.56%, lo que refuerza el interés aca-

démico por la ciberseguridad y los negocios para reducir una creciente preocupación de las organizaciones. La investigación indicó a EE.UU. con más producción científica, seguido de Reino Unido, y China. El estudio mostró las palabras claves *cybersecurity, machine learning, e internet of things* con más ocurrencias. Otros hallazgos revelaron Business Horizons como la principal revista, y los autores Kappelman, Maurer, y Torres como más relevantes. Como afiliaciones principales están Indiana University y la University North Texas. Además, el mapa temático entre 2018 y 2022, indicó que las palabras business, cybersecurity, y security se encuentra entre los temas motores y básicos, y *las* palabras *study, risk y organizations* como temas motores y nicho.

Como contribuciones teóricas, el estudio avanzó la frontera del conocimiento al reducir las brechas identificadas para minimizar los riesgos cibernéticos. Asimismo, la revisión bibliométrica permitió determinar la estructura intelectual y conocer el frente de investigación sobre ciberseguridad y negocios. Además, la investigación profundizó los estudios que relacionan ciberseguridad y negocios, con los ODS. Por fin, el estudio presentó una metodología de revisión bibliométrica que puede ser aplicada por otros investigadores. Como contribuciones prácticas, la investigación amplió la discusión sobre ciberseguridad y negocios que puede mejorar los análisis de gestores y responsables políticos en la toma de decisiones. Además, el estudio pretende crear conciencia entre los tomadores de decisiones sobre ciberseguridad y generar impacto positivo en la sociedad.

Otros hallazgos indicaron como tendencias enterprises, features, y models. En esta dirección, futuras líneas de investigación pueden profundizar estudios sobre ciberseguridad y aplicar algoritmos para reducir los riesgos en los procesos de decisión. En este caso, los autores proponen la aplicación de modelos de la Lógica Borrosa (Zadeh, 1965) que combinen los elementos de relación, asignación, agrupación, ordenación (Gil-Aluja, 1999). Finalmente, como principal mérito científico, el estudio fue innovador al realizar una revisión bibliométrica sobre ciberseguridad y negocios. Además, los autores buscaron sensibilizar a los gestores y responsables políticos sobre los riesgos

cibernéticos, y cómo la ciberseguridad puede impactar positivamente en los ODS 8 y 9.

Agradecimientos

Los autores agradecen a la Real Academia de Ciencias Económicas y Financieras, a la Cátedra UB-Fundación Mutua Madrileña sobre sostenibilidad empresarial, y a la CENTRUM Católica Graduate Business School.

Investigación apoyada por Red Sistemas Inteligentes y Expertos Modelos Computacionales Iberoamericanos (SIEMCI), proyecto número 522RT0130 en Programa Iberoamericano de Ciencia y Tecnología para el Desarrollo (CYTED).

Referencias

Abeshu, A., & Chilamkurti, N. (2018). Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing. IEEE Communications Magazine, 56(2), 169–175. https://doi.org/10.1109/MCOM.2018.1700332

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. Computers & Security, 101, 102122. https://doi.org/10.1016/j.cose.2020.102122

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, 144–166. https://doi.org/10.1016/j.cose.2018.01.001

Aria, M., & Cuccurullo, C. (2017). bibliometrix : An R-tool for comprehensive science mapping analysis. Journal of Informetrics, 11(4), 959–975. https://doi.org/10.1016/j.joi.2017.08.007

Babiceanu, R. F., & Seker, R. (2016). Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and futu-

re outlook. Computers in Industry, 81, 128–137. https://doi.org/10.1016/j.compind.2016.02.004

Barcellos-Paula, L., de La Vega, I., & GilČLafuente, A. M. (2022). Bibliometric review of research on decision models in uncertainty, 1990–2020. International Journal of Intelligent Systems, 37(10), 7300–7333. https://doi.org/10.1002/int.22882

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. Computers & Security, 89, 101677. https://doi.org/10.1016/j.cose.2019.101677

Bresniker, K., Gavrilovska, A., Holt, J., Milojicic, D., & Tran, T. (2019). Grand Challenge: Applying Artificial Intelligence and Machine Learning to Cybersecurity. Computer, 52(12), 45–52. https://doi.org/10.1109/MC.2019.2942584

Cobo, M. J., López-Herrera, A. G., Herrera-Viedma, E., & Herrera, F. (2011). An approach for detecting, quantifying, and visualizing the evolution of a research field: A practical application to the Fuzzy Sets Theory field. Journal of Informetrics, 5(1), 146–166. https://doi.org/10.1016/j.joi.2010.10.002

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in Industry, 114, 103165. https://doi.org/10.1016/j.compind.2019.103165

Croese, S., Green, C., & Morgan, G. (2020). Localizing the Sustainable Development Goals Through the Lens of Urban Resilience: Lessons and Learnings from 100 Resilient Cities and Cape Town. Sustainability, 12(2), 550. https://doi.org/10.3390/su12020550

Ghobakhloo, M. (2020). Determinants of information and digital technology implementation for smart manufacturing. International Journal of Production Research, 58(8), 2384–2405. https://doi.org/10.1080/00207543.2019.1630775

Gil-Aluja, J. (1999). Elements for a Theory of Decision in Uncertainty (Vol. 32). Springer US. https://doi.org/10.1007/978-1-4757-3011-1

Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (2019). Health Care and Cybersecurity: Bibliometric Analysis of the Literature. Journal of Medical Internet Research, 21(2), e12644. https://doi.org/10.2196/12644

Kappelman, L., Torres, R., McLean, E. R., Maurer, C., Johnson, V. L., Snyder, M., & Guerra, K. (2022). The 2021 SIM IT Issues and Trends Study. MIS Quarterly Executive, 21(1), 75–114. https://doi.org/10.17705/2msqe.00060

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. Journal of Contemporary Criminal Justice, 37(4), 480–501. https://doi.org/10.1177/10439862211027986

Kluczek, A., Gladysz, B., Buczacki, A., Krystosiak, K., Ejsmont, K., & Palmer, E. (2023). Aligning sustainable development goals with Industry 4.0 for the design of business model for printing and packaging companies. Packaging Technology and Science, 36(4), 307–325. https://doi.org/10.1002/pts.2713

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection, 9, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

Kosmowski, K. T., Piesik, E., Piesik, J., & ČiwiČski, M. (2022). Integrated Functional Safety and Cybersecurity Evaluation in a Framework for Business Continuity Management. Energies, 15(10), 3610. https://doi.org/10.3390/en15103610

Leng, J., Ye, S., Zhou, M., Zhao, J. L., Liu, Q., Guo, W., Cao, W., & Fu, L. (2021). Blockchain-Secured Smart Manufacturing in Industry 4.0: A Survey. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51(1), 237–252. https://doi.org/10.1109/TSMC.2020.3040789

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Manuel, D.-D., Carmona-Murillo, J., Cortes-Polo, D., & Rodriguez-Perez, F. J. (2022). CyberTOMP: A Novel Systematic Framework to Manage Asset-Focused Cybersecurity From Tactical and Operational Levels. IEEE Access, 10, 122454–122485. https://doi.org/10.1109/ACCESS.2022.3223440

Naffa, H., & Fain, M. (2020). Performance measurement of ESG-themed megatrend investments in global equity markets using pure factor portfolios methodology. PLOS ONE, 15(12), e0244225. https://doi.org/10.1371/journal.pone.0244225

Ngoc Thach, N., Thanh Hanh, H., Ngoc Huy, D. T., Gwozdziewicz, S., Viet Nga, L. T., & Thanh Huong, L. T. (2021). Technology Quality Management of the Industry 4.0 and Cybersecurity Risk Management on Current Banking Activities in Emerging Markets - The Case in Vietnam. International Journal for Quality Research, 15(3), 845–856. https://doi.org/10.24874/IJQR15.03-10

Nishant, R., Kennedy, M., & Corbett, J. (2020). Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda. International Journal of Information Management, 53, 102104. https://doi.org/10.1016/j.ijinfomgt.2020.102104

Noyons, E. C. M., Moed, H. F., & Luwel, M. (1999). Combining mapping and citation analysis for evaluative bibliometric purposes: A bibliometric study. Journal of the American Society for Information Science, 50(2), 115–131. https://doi.org/10.1002/(SICI)1097-4571(1999)50:2<115::AID-ASI3>3.0.CO;2-J

Rashid, Z., Noor, U., & Altmann, J. (2021). Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem. Future Generation Computer Systems, 124, 436–466. https://doi.org/10.1016/j.future.2021.05.033

Robles-Gomez, A., Tobarra, L., Pastor-Vargas, R., Hernandez, R., & Haut, J. M. (2021). Analyzing the Users' Acceptance of an IoT Cloud Platform Using the UTAUT/TAM Model. IEEE Access, 9, 150004–150020. https://doi.org/10.1109/ACCESS.2021.3125497

Shah, S. (2020). The Technological Impact of COVID-19 on the Future of Education and Health Care Delivery. Pain Physician, 4S;23(8;4S), S367–S380. https://doi.org/10.36076/ppj.2020/23/S367

United Nations. (2018). Sustainable Development Goals. https://www.un.org/sustainabledevelopment/sustainable-development-goals/

Zadeh, L. A. (1965). Fuzzy sets. Information and Control, 8(3), 338–353. https://doi.org/10.1016/S0019-9958(65)90241-X

Zupic, I., & Čater, T. (2015). Bibliometric Methods in Management and Organization. Organizational Research Methods, 18(3), 429–472. https://doi.org/10.1177/1094428114562629

CYBER-ECONOMY: LE PARADOXE DE LA ROUMANIE

Dr. Valeriu Ioan-Franc[1]
Académico Correspondiente por Rumanía de la Real Academia de Ciencias Económicas y Financieras

Dr. Andrei-Marius Diamescu[2]
Institut National de Recherches Economiques «Costin C. Kirițescu», Académie Roumaine

Abstract

At a time when the effects of the almost15 years ago financial crisis haven't yet had their full impact, when the hesitant exist from the COVID -19 pandemic has left us searching for a new normal so little glimpsed and weakly supported by the Community Resilience and Recovery Program, a new crisis is on the horizon. Called globalisation through development, overlapped on the energy crisis and the sought-after but increasingly distant decarbonisation crisis, cyber-economy is among major attempts placed before the economic and social. The authors show, as they previously have[3,4] (Ioan-Franc, Diamescu 2022, 2023), starting from the uncontested opportunities for development offered by computerization/digitization (artificial

1 Directeur général adjoint de l'Institut National de Recherches Economiques «Costin C. Kirițescu» de l'Académie Roumaine, Bucarest, Calea 13 Septembrie, no. 13, tél.: +4023182438, e-mail: cide90@gmail.com.

2 Chercheur senior, Institut National de Recherches Economiques «Costin C. Kirițescu» de l'Académie Roumaine, Bucarest, Calea 13 Septembrie, no. 13, tél.: 040735317171, e-mail : dandreimarius@yahoo.com.

3 Ioan-Franc, V.; Diamescu, A.-M., 2022 - *Ne «jouons» plus au Dieu!*, Soluciones económicas y tecnológicas a la degradación del ecosistema del planeta, Real Academia de Ciencias Económicas y Financieras - RACEF, Barcelona, pp. 83-100.

4 Ioan-Franc, V.; Diamescu, A.-M., 2023 - *L'intelligence artificielle* - opportunités, responsabilité, inquiétudes, Synthèse du discours prononcé à la réunion RACEF-BEN avec l'Université de Kragujevac – Serbia, 23 avril 2023.

intelligence), drawing attention to the responsibility, the challenges that the present brings to the near future and not only.

The authors' concerns are about a new social fragmentation, between generations and their capabilities, between the abilities gained in school and the knowledge provided by school. In the context of the current meeting of RACEF – Barcelona Economic Network, the ways in which Romania answers the mentioned challenges are approached. The conclusion of our intervention in the form of describing the Romanian paradox in the matter: a country that is a net exporter of IT intelligence worldwide with a hard to understand internal gap in the same area.

1. Quelques considérations générales

Souvent appelée comme être en réalité **la quatrième révolution industrielle**, et fréquemment comparée, compte tenu des grandes implications socio-économiques et de ses conséquences, avec le moteur à vapeur, l'introduction simultanée généralisée dans la vie économique et sociale de l'intelligence artificielle (IA) est aujourd'hui *une réalité qui semble effrayer plutôt que réjouir*.

L'euphorie initiale, générée par l'apparition du *« téléphone sans fil »* et, peu après, de l'Internet, qui a brusquement démantelé, pourrait-on dire, les distances entre les personnes et ouvert un large accès à l'information (mondialisation), est aujourd'hui visiblement remplacée par une série de préoccupations, mais aussi par de confusions.

Nous sommes conscients que l'approche exhaustive de ces « *ambiguïtés* » est pratiquement impossible, tout comme, du moins à notre avis, il est impossible d'harmoniser les perspectives sur l'utilisation de l'intelligence artificielle entre ses « *promoteurs* » et ses « *bénéficiaires* »!

En tant qu'économistes et chercheurs, nous devrions, au moins apparemment, nous positionner dans la loge des partisans des «*promoteurs*», mais c'est précisément pour cette raison que nous avons choisi d'élargir la portée de nos réflexions dans le domaine des «*bénéficiaires*», en espérant que de cette façon nous nous rapprocherons, sinon à la réalité, au moins à l'illusion d'une approche objective.

Admettant qu'aujourd'hui la présence de l'intelligence artificielle dans la vie quotidienne, sous diverses formes et degrés de complexité, a atteint le niveau critique pour être considérée comme un réel phénomène économique (**cyber-economy**) et social, nous ressentons le besoin de partager, dès le début, deux observations / questions qui nous préoccupent :

1.1. Une première observation est que **le rythme auquel l'intelligence artificielle/cyber-economy se développe actuellement dépasse clairement sa capacité d'absorption/adaptation/intégration sociale.**

Selon un rapport de l'Université de Stanford en Californie, **le nombre de brevets d'IA a été multiplié par 30 entre 2015 et 2021[5].**

Juste un exemple, la nouvelle application ChatGPT, lancée à la fin du mois de novembre de l'année dernière, a atteint un million d'utilisateurs au cours des cinq premiers jours et a atteint, en janvier 2023, 100 millions d'utilisateurs, devenant ainsi l'application Web à la croissance la plus rapide jamais enregistrée[6].

5 Apud. Ionescu V, The Guardian : La révolution industrielle menée par l'intelligence artificielle menace les emplois de la classe moyenne, 19 Fév. 2023 sur https://cursdeguvernare.ro/the-guardian-revolutia-industriala-antrenata-de-inteligenta-artificiala-ameninta-locurile-de-munca-ale-clasei-de-mijloc.html

6 Apud. Ionescu V, Experts: ChatGPT peut conduire à des escroqueries sentimentales , 19 Fév.. 2023, sur https://cursdeguvernare.ro/experti-chatgpt-poate-duce-la-aparitia-escrocheriilor-sentimentale.html

D'autre part, **l'Indice de l'économie et de la société numérique (DESI) 2022** nous montre qu'en Europe, même si 87% de la population âgée de 16 à 74 ans utilise Internet, seuls **54% possèdent au moins des compétences numériques de base**. Cette réalité, pas du tout encourageante, est également confirmée par le degré d'intégration des technologies numériques dans les entreprises, où, en 2021, seulement 55% de toutes les petites et moyennes entreprises ont atteint un niveau de base, 14% ont utilisé des systèmes Big Data et **seulement 8% ont utilisé l'intelligence artificiell**e[7].

L'écart entre le rythme de développement de la **cyber-economy** et la capacité de la société à utiliser les nouvelles technologies a été très bien mis en évidence depuis la fin de 2021, grâce à l'enquête **Dentons** (cabinet d'avocats multinational de premier plan, possédant une solide expertise dans des domaines comme la protection des données personnelles, la confidentialité et les droits des consommateurs ou la propriété intellectuelle) parmi plus de 200 leaders de l'environnement commercial international.[8] Selon l'enquête, les gens d'affaires reconnaissent les nombreux avantages de la cyber-economy (gagner du temps en automatisant les processus, générer rapidement l'information nécessaire pour prendre des décisions ou réduire le nombre d'erreurs humaines dans le traitement des données disponibles), mais en même temps, ils ont exprimé de graves préoccupations, notamment :

- seulement 55% des entreprises ont des politiques de protection des données personnelles et non personnelles;

- seules 19 % des entreprises disposent d'une stratégie ou de lignes directrices sur l'utilisation de l'IA, ce qui signifie que la *technologie est mise en œuvre sans tenir compte des risques, de la législation appli-*

7 Commission européenne, Indice de L'Économie numérique et de la Société (DESI) 2022; Chapitres thématiques, sur https://digital-strategy.ec.europa.eu/en/policies/desi

8 Apud. Lowe A, Dentons Sondage sur l'IA : principales constatations, dans Affaires Passées au Numérique, Déc. 2021 sur https://www.businessgoing.digital/dentons-ai-survey-key-findings/

cable pertinente, ou des contrôles internes nécessaires pour s'assurer qu'elle est correctement mise en œuvre et gérée ;

- 80 % des chefs d'entreprise ont mentionné l'incertitude au sujet du département ou des personnes responsables des décisions et des omissions prises par les systèmes d'IA;

- 57 % d'entre eux s'inquiètent du *risque de discrimination* découlant de l'utilisation des systèmes d'IA;

- selon le domaine juridique, entre 55% et 75% des personnes interrogées ne connaissent pas la législation nationale applicable aux systèmes d'IA, et 63% ne savent pas quel organisme public réglemente ce domaine;

- **les entreprises s'attendent à ce que les organismes de réglementation fournissent de toute urgence des protections pour l'utilisation de l'IA par rapport à la vie privée (61 %), la protection des consommateurs (52 %), la responsabilité criminelle (46 %) et la propriété intellectuelle (45 %).**

Résumant les résultats de l'enquête Dentons, on peut dire que les **États** (y compris les syndicats d'État) **n'ont pas fait leur devoir**, étant responsables, avec d'autres facteurs, objectifs et subjectifs, des écarts induits dans la société par la **cyber-economy**. En d'autres termes : **l'ingénierie technologique a dépassé l'ingénierie sociale** !

C'est une réalité ? Oui, et une réalité dure, très bien soulignée par l'écrivain et journaliste roumain réputé, l'ancien ministre de la Culture, Alexandru Mironov, qui croit que « *notre société, telle qu'elle est, ne résistera pas à la pénétration de l'intelligence artificielle* » et, continue à faire des prévisions, « *en 2035, nous pourrons voir que les murs des salles de classe disparaîtront. Bientôt, une littérature policière apparaîtra, parce que, comme les choses sont*

entrées dans cette voie, elles ne seront pas en mesure de s'arrêter. Ce robot (ChatGPT – n.n.), qui est composé de bits et n'a pas d'autre consistance, s'est mis en route, parcourt toutes les bibliothèques du monde, tous les laboratoires de personnes intelligentes et devient (certains croient, n.n. !) de plus en plus intelligent. ***Nous ne savons pas ce qu'il voudra faire demain.*** *»*[9].

1.2. La deuxième observation que nous voulons faire est en fait une question : **les besoins sociaux déterminent-ils/formulent-ils les exigences de la cyber-economy, ou la cyber-economy force-t-elle l'émergence de nouveaux besoins et les résout-elle?**

Apparemment, la réponse à cette question est simple et établie : l'IA est née de la nécessité de simplifier le travail de l'homme, de soulager l'individu humain d'une série d'activités, généralement itératives, de sorte que sa vie serait « *plus facile* »!

Immédiatement, de nombreux autres partisans de l'IA sont apparus, soulignant les nombreux avantages qu'elle apporte à l'économie, mais pas seulement, tels que : augmenter la productivité, simplifier les flux de production et de les normaliser, améliorer la qualité des produits, réduire les coûts de main-d'œuvre, etc., qui sont dans une large mesure vraie. Le profit (encore une fois le profit!) unitaire et global, il a augmenté. Mais est-ce suffisant ?!

Tous ces arguments ont fait aujourd'hui environ 60% des grandes entreprises, en particulier les multinationales, utilisent l'IA dans leur activité, y compris dans les processus décisionnels[10].

9 Apud. Dicu A., *Dans un avenir pas du tout « SF ». Les robots nous remplaceront au travail. La prédiction d'Alexander Mironov : « Nous ne résisterons pas à l'émancipation de l'intelligence artificielle! »*, 11.fév,2023, sur https://www.fanatik.ro/intr-un-viitor-deloc-sf-robotii-ne-vor-inlocui-la-serviciu-predictiile-lui-alexandru-mironov-nu-vom-rezista-in-fata-emanciparii-inteligentei-artificiale-20305403

10 Dentons, *Guide de L'Intelligence Artificielle 2022 Le parcours de L'IA – ouvrir les yeux sur les possibilités et les risques*, Déc. 2021, sur https://www.acc.com/sites/default/files/resources/upload/Dentons

L'expérience acquise dans l'utilisation toujours croissante de l'IA dans le contexte des activités économiques (**cyber-economy**) semble avoir « *calmé* » l'enthousiasme initial. Ce qui hier semblait la solution parfaite aux défis économiques contemporains, que l'on parle de gestion économique ou des activités de production elles-mêmes, aujourd'hui nous oblige à réévaluer l'impact et impose la nécessité d'une réglementation dans ce domaine qui connaît un développement accéléré.

« *Les chefs d'entreprise au niveau mondial commencent à se poser de sérieuses questions sur la responsabilité de la bonne gouvernance, de la réglementation et de la conformité (dans l'utilisation de l'I.A. – n.a.). Nous devons de toute urgence entamer un dialogue sur les contrôles nécessaires pour protéger les entreprises, les clients, les actionnaires et les communautés* », a déclaré Giangiacomo Olivo, co-président de Dentons Europe pour la confidentialité des données, la cybersécurité, la propriété intellectuelle et la technologie[11].

Les recherches de Dentons, comme nous l'avont déjà dit, ont révélé de multiples dysfonctionnements et même des risques liés à l'utilisation de l'IA en dehors d'un cadre juridique/réglementaire approprié et, ce qui est très important, en consensus au niveau de la communauté internationale, étant donné la pertinence transfrontalière des systèmes utilisant l'IA.

C'est pourquoi il est nécessaire de créer d'urgence un système d'« **algoréthique** » – un terme créé par l'association des mots éthiques et de l'algorithme – à la base de l'IA – afin que « *les considérations morales deviennent partie intégrante du développement des technologies de l'IA [...] et les bons contrôles peuvent être mis en œuvre*. »[12].

11 *** *Les chefs d'entreprise mondiaux expriment leurs principales préoccupations concernant l'utilisation de L'Intelligence Artificielle,* Jan. 2022, sur https://www.dentons.com/en/about-dentons/news-events-and-awards/news/2022/january/global-business-leaders-voice-major-concerns-over-the-use-of-artificial-intelligence

12 Idem 5

2. Le paradoxe de la Roumanie

La nécessité d'une réglementation dans le domaine de l'utilisation de l'IA, y compris la **cyber-economy**, a été très bien exprimée par Leonard Azamfirei, recteur de l'Université de Médecine, Pharmacie, Sciences et Technologie de Târgu-Mureş : « *Dans toute cette frénésie de développer de nouvelles technologies qui intègrent l'intelligence artificielle, qui a le temps de penser aux bonnes mesures algoréthiques, de contrôle et d'équilibre ? Les géants de la technologie sont trop peu enclins aux réserves éthiques quant à l'exploitation intégrale des nouvelles technologies, mais les États doivent réagir sur le plan législatif, et imposer des considérations morales comme partie intégrante du processus de développement d'outils avancés de l'intelligence artificielle*. »[13]

En paraphrasant le logo d'une ancienne campagne nationale de promotion du tourisme, on peut dire que, même en termes de **cyber-economy (CE)**, la Roumanie est « *toujours surprenante* », voire contradictoire !

Alors que L' Administration Internationale du Commerce (AIC) du Département du Commerce des États-Unis caractérise, dans le guide de pays publié le 27.07.2022, la composante Technologies de l'Information et des Communications (IT&C) de l'économie roumaine est « un secteur industriel de meilleure perspective pour ce pays »,[14] l'Indice Européen de l'Économie et de la Société numériques (DESI) 2022, développé par la Commission Européenne, place notre pays au dernier rang -27- au sein de l'Union Européenne[15].

Au-delà des classements généraux, les évaluations des composantes cyber-economy analysées dans notre pays révèlent une **évolution du secteur**

13 https://stirileprotv.ro/stiri/ilikeit/rector-umfst-statul-trebuie-sa-impuna-consideratii-morale-in-dezvoltarea-ia-exista-riscul-ca-omul-sa-piarda-controlul.html

14 https://www.trade.gov/country-commercial-guides/romania-information-communications-technology-ict

15 Commission Européenne, L'Indice de L'Ëconomie et de la Société Numériques (DESI) 2022; Chapitres thématiques, sur https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

que nous appellerions « non linéaire », car elle met en évidence un développement conjoncturel qui s'est produit en l'absence d'une stratégie conforme aux politiques européennes et inégale, comme le reconnaît le DESI 2022[16].

Le souci généralement réduite des pouvoirs publics, tant centraux que locaux, d'éduquer et de faciliter l'accès du grand public aux services numériques est plus qu'évident, si l'on considère les résultats publiés par la Commission Européenne à la suite de son évaluation, à la fin de l'année dernière :

4 Services publiques numériques	**Roumanie**		**UE points**
	place	**points**	
DESI 2022	**27**	**21,0**	**67,3**

	Roumanie			**UE**
	DESI 2020	**DESI 2021**	**DESI 2022**	**DESI 2022**
4a1 Utilisateurs des solutions de e-gouvernement % parmi les utilisateurs de l'internet	15% 2019	16% 2020	17% 2021	65% 2021
4a2 Formulaires complétés d'avance Points (0-100)	Non applicable	Non applicable	19 2021	64 2021
4a3 Services publics numériques pour les citoyens Points (0-100)	Non applicable	Non applicable	44 2021	75 2021
4a4 Services publics numériques pour les entreprises Points (0-100)	Non applicable	Non applicable	42 2021	82 2021
4a5 Dates ouvertes % des points maximums	Non applicable	Non applicable	76% 2021	81% 2021

Source : https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

Les écarts importants entre les résultats de la Roumanie et la moyenne de l'UE parlent d'eux-mêmes et, en même temps, exigent une action immédiate et coordonnée pour récupérer le retard. Le 3 juin 2021, la politique publique nationale dans le domaine de l'e-gouvernement a été adoptée, et définit

16 Idem 8

simultanément une vision et une feuille de route pour la numérisation des services publics au cours des dix prochaines années, ainsi qu'un mécanisme de suivi, évaluer et ajuster périodiquement le rythme et les étapes à suivre. Les objectifs proposés, que l'on peut qualifier de non seulement nécessaires, mais aussi obligatoires pour le recouvrement des retards, sont loin d'être atteints.

Dans une approche objective de l'étape dans laquelle nous sommes, il est plus facile de comprendre que, alors que **la Roumanie est un leader européen et se classe 6 dans le monde en termes de nombre de spécialistes IT certifiés par 1,000 habitants**, à un taux supérieur à celui des États-Unis ou de la Fédération de Russie[17], « *le pays a pris du retard dans un certain nombre d'indicateurs de la taille du capital humain, avec* ***un niveau très faible*** *de compétences numériques de base par rapport à la moyenne de l'UE* »[18].

1 Capital humain	**Roumanie**		**UE points**
	place	**points**	
DESI 2022	**27**	**30,9**	**45,7**

	Roumanie			**UE**
	DESI 2020	**DESI 2021**	**DESI 2022**	**DESI 2022**
1a1 Compétences numériques au moins de base % des personnes	Non applicable	Non applicable	28% 2021	54% 2021
1a2 Compétences numériques au-delà du niveau élémentaire % des personnes	Non applicable	Non applicable	9% 2021	26% 2021

continue

17 https://www.trade.gov/country-commercial-guides/romania-information-communications-technology-ict

18 Commission Européenne, L'Indice de L'Ëconomie et de la Société Numériques (DESI) 2022; Chapitres thématiques, sur https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

1a3 Compétences numériques au moins de base % des personnes	Non applicable	Non applicable	41% 2021	66% 2021
1b1 Spécialistes dans le domaine ITC % des personnes âgées entre 15 et 74 ans	2,3% 2019	2,4% 2020	2,6% 2021	4,5% 2021
1b2 Femmes spécialistes dans le domaine ITC % des spécialistes dans le domaine ITC	23,5% 2019	26,2% 2020	26% 2021	19,1% 2021
1b3 Entreprises délivrant une formation dans le domaine ITC % des entreprises	6% 2019	6% 2020	6% 2020	20% 2020
1b4 Absolvents dans le domaine ITC % parmi les absolvents	5,8% 2018	6,3% 2019	6,7% 2020	3,9% 2020

Sursa: https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

Apparemment antagonistes, les deux déclarations ne deviennent explicables que lorsque, à partir des analyses concernant le capital humain, nous remarquons que, malgré les faibles compétences numériques générales, la Roumanie se classe 4 dans l'UE, en termes de nombre de diplômés dans le domaine IT&C!

Mais cet intéressant *tableau de bord* du capital humain révèle également une autre dimension, qui n'est pas du tout gratifiante : *la polarisation* ou, peut-être mieux dit, *la concentration de compétences numériques avancées au sein des entreprises dans le domaine*, qui offrent des salaires motivants (pour souligner qu'en Roumanie, les spécialistes IT bénéficient également d'autres facilités importantes, telles que l'exonération totale de l'impôt sur le revenu!) par rapport aux salaires moyens dans notre pays et qui, dans la plus grande mesure, « ***exporte*** » leurs résultats, **sans avantages directs pour l'ensemble de la population du pays**.

Cette réalité est d'ailleurs indirectement confirmée par le guide pays du Département du Commerce des Etats-Unis, selon lequel **les 50 grandes entreprises du secteur présentes en Roumanie ont quadruplé leurs affaires et équipes ces dernières années**[19].

Il convient également de noter que, sur l'ensemble des personnes âgées de 15 à 74 ans ayant un emploi, **seulement 2,6 % sont des spécialistes en IT&C**, contre 4,5 % de la moyenne européenne – encore une fois, apparemment contradictoire étant donné qu'un employé IT&C gagne, en moyenne, plus du double du salaire moyen dans l'économie (env. 1.400 euro/mois), et le personnel dans le domaine du développement de logiciels bénéficient des salaires les plus élevés dans le pays (en moyenne, 1.750 euro/mois)[20]!

Malgré tous ces avantages salariaux, les spécialistes de l'Association des Employeurs de L'Industrie du Logiciel et des Services (ANIS) comprennent que dans notre pays il y a une pénurie importante de spécialistes, à savoir plus de 10,000. « *Le gouvernement fait très peu pour lutter contre cette pénurie de travailleurs qualifiés et, par conséquent, il est très important de tenir compte du déficit des employés qui ne sont pas qualifiés, le secteur compte de plus en plus sur ses propres mesures (formation professionnelle locale) pour répondre à la demande*. »[21]

19 "*La Roumanie […] abrite un nombre impressionnant d'entreprises technologiques internationales (dont Amazon, HP, IBM, Microsoft et Oracle, etc.), 50 des plus grandes entreprises technologiques présentes en Roumanie ayant quadruplé leurs activités et leurs équipes au cours des dernières années.*" apud https://www.trade.gov/country-commercial-guides/romania-information-communications-technology-ict

20 https://www.trade.gov/country-commercial-guides/romania-information-communications-technology-ict

21 Apud. Radu C., *Roumanie: Un « champion caché » de la numérisation ? Que sait ChatGPT et que savent les spécialistes ? Une conversation avec l'intelligence artificielle sur la numérisation en Roumanie, 12 février 2023 sur* https://economedia.ro/romania-un-campion-ascuns-al-digitalizarii-ce-stie-chatgpt-si-ce-stiu-specialistii-o-conversatie-cu-artificial-intelligence-despre-digitalizarea-in-romania.html#.ZCvktntBy3A

La cause de ces « écarts » devient identifiable lorsqu'on analyse le degré d'intégration dans l'économie roumaine du numérique, un indicateur qui place de nouveau notre pays au bas du classement européen, avec un score (15,2) à moins de la moitié du score moyen enregistré dans les pays de l'UE (36,1)[22]!

3 Intégration de la technologie numérique	**Roumanie**		**UE points**
	place	**points**	
DESI 2022	**27**	**15,2**	**36,1**

	Roumanie			**UE**
	DESI 2020	**DESI 2021**	**DESI 2022**	**DESI 2022**
3a1 EPM ayant au moins un niveau de base d'intensité numérique % des EPM	Non applicable	Non applicable	22% 2021	55% 2021
3b1 Échange numérique d'informations % des entreprises	23% 2019	23% 2019	17% 2021	38% 2021
3b2 Platformes de communication sociale % des entreprises	8% 2019	8% 2019	12% 2021	29% 2021
3b3 Grands volumes de dates % des entreprises	11% 2018	5% 2020	5% 2020	14% 2020
3b4 Technologie de type cloud % des entreprises	Non applicable	Non applicable	11% 2021	34% 2021
3b5 IA % des entreprises	Non applicable	Non applicable	1% 2021	8% 2021
3b6 ITC pour la durabilité de l'environnement % des entreprises qui ont une intensité moyenne/élevée des actions vertes par ITC	Non applicable	68% 2021	68% 2021	66% 2021

continue

22 Commission Européenne, L'Indice de L'Économie et de la Société Numériques (DESI) 2022; Chapitres thématiques, sur https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

3b7 Factures électroniques % des entreprises	20% 2018	17% 2020	17% 2020	32% 2020
3c1 EPM qui effectuent des ventes onlines % des EPM	11% 2019	17% 2020	12% 2021	18% 2021
3c2 Chiffres d'affaires du commerce numérique % de la chiffre d'affaires de EPM	5% 2019	8% 2020	7% 2021	12% 2021
3c3 Ventes online transfrontalières % des EPM	6% 2019	6% 2019	4% 2021	9% 2021

Source: https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

C'est ainsi que, malgré les politiques publiques de numérisation lancées au niveau gouvernemental, presque tous les indicateurs sont bien en dessous de la moyenne de l'UE et, ce qui est plus alarmant, ils ont stagné ou même diminué en 2021-2022.

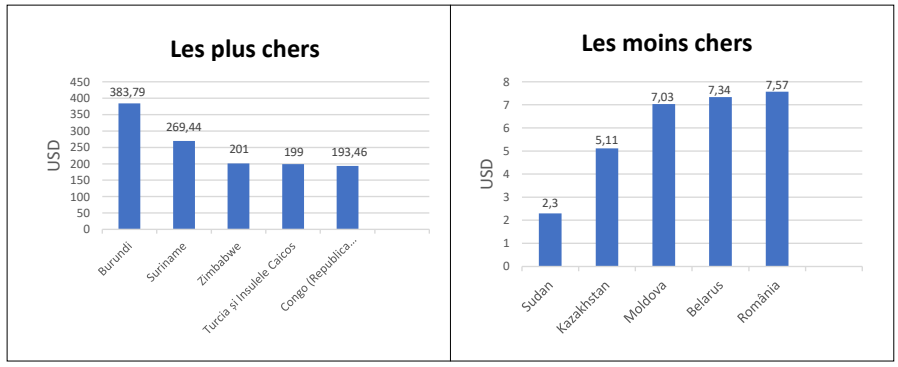
La situation est encore plus préoccupante lorsqu'il s'agit de l'adoption de technologies de pointe comme celle de type cloud ou l'intelligence artificielle. Cumulativement, tous ces « retards » placent la Roumanie face à un véritable défi en ce qui concerne l'objectif de la décennie numérique européenne, à savoir que d'ici 2030, 75 % des entreprises devraient utiliser la technologie de type cloud, les grands volumes de données et l'intelligence artificielle.

L'objectif, en ce moment, est assez difficile à atteindre dans une économie comme celle de la Roumanie, où la perspective d'une exploitation correcte de la cyber-economy ne montre qu'un *réel potentiel de développement dans ce domaine*. Un potentiel, il est vrai, justifié non seulement par le capital humain que nous avons, mais aussi par le niveau de connectivité atteint qui, même s'il est encore inférieur à la moyenne européenne, nous place sur une place honorable (15) au sein de l'UE[23].

23 Commission Européenne, L'Indice de L'Ëconomie et de la Société Numériques (DESI) 2022; Chapitres thématiques, sur https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

En outre, l'année dernière (2022) **la Roumanie a grimpé trois positions dans le classement mondial des pays avec l'internet le moins cher, atteignant la 5-ème place**, avec un prix moyen de 35 ron (env. 7 euros) par mois pour un forfait internet haut débit!

Les cinq pays les plus chers et les cinq pays les moins chers au monde, en termes de coût mensuel moyen du haut débit



Source: https://www.cable.co.uk/broadband/pricing/worldwide-comparison/

Malheureusement, comme le note le profil pays de l'Indice Européen de l'Économie et de la Société Numériques (DESI) 2022, « *Le plus grand défi auquel la Roumanie est confrontée, en termes de connectivité est d'améliorer le taux global d'utilisation des services fixes à large bande, qui reste à 66%, bien en dessous de la moyenne de l'UE (78%), malgré le faible coût des services à large bande et la couverture élevée des réseaux à très haute capacité (VHCN).* »

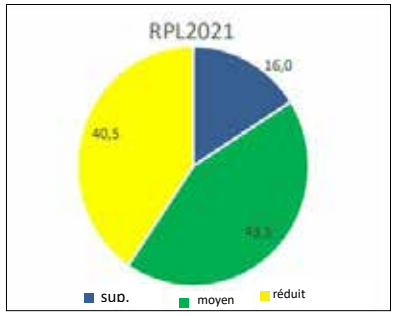
Cet immense « *défi* » a, à notre avis, une cause objective, confirmée par les résultats provisoires, publiés par l'Institut National de la Statistique, pour le Recensement de la Population et du Logement, l'étape 2021[24]: **l'approfon-**

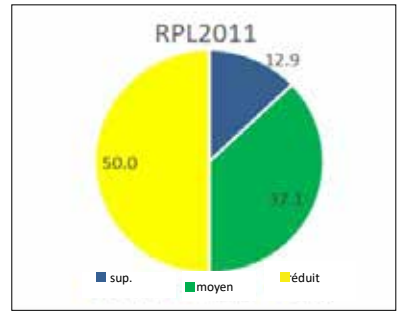
24 Commission Européenne, L'Indice de L'Ëconomie et de la Société Numériques (DESI) 2022; Chapitres thématiques, sur https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

dissement du processus de vieillissement démographique, étant connu le fait qu'avec l'âge on diminue à la fois le niveau de motivation et la capacité naturelle d'acquérir et d'utiliser de nouvelles technologies.

Selon ce document, « *par rapport à il y a 10 ans […]* ***l'indice de vieillissement démographique a diminué de près de 20 points de pourcentage****, passant à 121,2 personnes âgées (65 ans et plus) pour 100 jeunes en 2021, comparativement à 101,8 en 2011* ».

Ces déséquilibres dans la structure par âge de la population du pays s'ajoutent au **pourcentage encore élevé de la population ayant un faible niveau d'éducation** (c'est-à-dire le niveau d'éducation primaire, secondaire ou sans diplôme d'études) qui, bien qu'il ait connu une amélioration au cours de la dernière décennie, **se trouve à 40%**.





Source: L'Institut National de la Statistique, communiqué de presse : Premières données provisoires pour le Recensement de la Population et du Logement, l'étape 2021, sur https://insse.ro/cms/sites/default/files/com_presa/com_pdf/cp-date-provizorii-rpl2021.pdf

La corroboration des deux indicateurs auxquels nous avons fait référence fournit simultanément une explication manifestement partielle du faible niveau des compétences numériques de base, mais aussi une image réaliste des défis que la Roumanie doit résoudre dans les prochains 7-8 ans, afin de combler l'écart par rapport à la moyenne européenne.

L'échec de la Roumanie à atteindre les objectifs de la Décennie Numérique Européenne est, en ce moment, impensable, car cela signifierait de facto la perte de compétitivité économique, étant donné que « *les technologies avancées de traitement de l'information et de communication, les stratégies avancées de leadership sont naturellement intégrées dans n'importe quel domaine socioéconomique, avec des avantages majeurs pour la qualité des produits et, implicitement, pour la qualité de la vie. […] Le fort potentiel d'innovation permettra un changement de paradigme dans les systèmes de fabrication et, évidemment, une transformation radicale de l'économie numérique* »[25].

Le jour, anticipé par l'académicien Ioan Dumitrache depuis 10 ans, où « *le concept d'entreprise intelligente devient réalité* » **était hier** et a trouvé la Roumanie insuffisamment préparée, malgré son potentiel technique et novateur.

Toutefois, le rythme de développement enregistré ces dernières années par l'industrie IT&C est au moins « *encourageant* ». Selon l'Association des Employeurs de L'Industrie du Logiciel et des Services, ce secteur « *a connu une croissance exponentielle au cours des cinq dernières années, presque trois fois plus rapide (+17 %) que l'économie nationale (+6 %). La part de l'industrie IT&C s'est élevée à 13,6 milliards d'euros, soit environ 6,2 % du PIB de la Roumanie* »[26].

En même temps, en termes de scène des start-up IT, la Roumanie est vraiment un champion. Selon Konrad Adenauer Stiftung, « *en Roumanie, de nouvelles solutions et innovations sont constamment développées dans des*

25 Dumitrache I, *Cyber-phisical-systems (CPS) – un facteur clé dans l'économie du savoir et de l'innovation*, dans revue Roumaine d'Informatique et de Contrôle Automatique, vol. 23. No 4, 2013, p. 44 sur http://www.rria.ici.ro

26 Apud. Radu C., *La Roumanie: Un "champion caché" de la numérisation? Que sait ChatGPT etque savent les experts? Une conversation avec Artificial Intelligence sur la numérisation dans la Roumanie*, 12.fév.2023 sur https://economedia.ro/romania-un-campion-ascuns-al-digitalizarii-ce-stie-chatgpt-si-ce-stiu-specialistii-o-conversatie-cu-artificial-intelligence-despre-digitalizarea-in-romania.html#.ZCvktntBy3A

domaines tels que l'intelligence artificielle, l'automatisation, l'apprentissage automatique, etc. Dans des entreprises technologiques comme UiPath, Druid ou Fintech OS, de solides talents sont présents »[27].

A tout cela s'ajoute le marché **cyber-security** en Roumanie, caractérisé par le Département du Commerce des États-Unis, comme étant toujours émergent « *La Roumanie affiche le taux de travailleurs par habitant le plus élevé d'Europe dans ce secteur. Cependant, le marché de la cybersécurité en Roumanie est également ouvert aux acteurs étrangers, avec des fournisseurs américains (et pas seulement – n.a.) bien représentés*. »[28].

En reconnaissance de ses performances dans le domaine de la cybersécurité, Bucarest a été sélectionné par l'UE parmi les sept villes concurrentes et accueille, depuis 2021, le Centre européen de Compétences Industrielles, Technologiques et de Recherche. En plus de distribuer des fonds européens pour des projets de recherche sur la cybersécurité, le Centre a pour rôle de renforcer la résilience, la dissuasion et la réponse de l'Union Européenne aux cyberattaques, dans le but de sécuriser le Marché Unique Numérique (DSM) de L'UE.

À la performance de la Roumanie en matière de cybersécurité a contribué, tout d'abord, le fait que dans la plupart des grandes universités du pays, plus de 15 programmes de cybersécurité ont été développés sur des sujets allant de la cybersécurité des systèmes numériques, la cryptographie et les enquêtes numériques, jusqu'à l'apprentissage automatique et la sécurité des réseaux.

Encourageants sont également les objectifs dans le domaine **cyber-economy**, de l'utilisation de l'intelligence artificielle en général, que la Roumanie a proposé dans le cadre du Plan National de Redressement et de Résilience (PNRR) approuvé par le Conseil de l'UE du 28 octobre 2021, qui contribue à hauteur de 5,97 milliards d'euros (20,5 % de la dotation totale de la Rouma-

27 Idem 18

28 https://www.trade.gov/country-commercial-guides/romania-information-communications-technology-ict

nie) pour atteindre les objectifs numériques. De ce montant, la contribution la plus importante – 1.817 millions d'euros – a été allouée à la transformation numérique du secteur public, à la cybersécurité et à la connectivité (Composante 7), avec la composante 15 du Plan Éducation – avec une allocation de 1.129,5 millions d'euros, destinés à assurer le profil numérique des compétences des enseignants et à évaluer les compétences numériques lors des examens scolaires, mais aussi à garantir des normes pour équiper les écoles d'équipements et de ressources technologiques du domaine IT&C, adaptés à des fins éducatives.

3. Préoccupations justifiées

Comme tous les autres pays, comme le monde entier, il faudra veiller à contrôler la moralité de l'utilisation de l'intelligence artificielle et, implicitement, de la cyber-economy. Nous réitérons ici certains de nos points de vue, exprimés dans le même cadre généreux de débat ouvert et dûment défendus par la RACEF à l'École d'économie humaniste de Barcelone. Nous faisons référence à :

- l*a polarisation marquée de la société,* de la division des populations en *«spécialistes/initiés» et «analphabètes numériques»* ;

- ce type de «ségrégation» a des implications qui vont bien au-delà des questions d' « estime de soi », par exemple. En l'absence de mesures administratives efficaces, *les lacunes en matière de culture numérique* conduisent inévitablement à restreindre l'accès d'une grande partie de la population à de nombreux services publics, qu'il s'agisse de services administratifs, bancaires, de transport, de santé ou même d'éducation. Tous ces aspects se traduisent directement par une baisse de la qualité de vie des citoyens, alors que l'objectif affiché des technologies TIC, de l'intelligence et de l'économie numérique est précisément de l'augmenter !

- *la concentration des données et des informations véhiculées par les systèmes d'IA entre les mains de quelques entreprises/institutions* capables non seulement d'échapper au contrôle de l'État, mais même d'exercer un contrôle sur les institutions démocratiques ;

- *le pouvoir extraordinaire que ces acteurs ont acquis, en combinant la puissance financière et l'information* qu'ils détiennent, nous oblige aujourd'hui, plus que jamais, à réfléchir à la question suivante : *dans le contexte actuel, la démocratie, dans sa forme grecque antique et séculaire, est-elle encore capable de respecter ses principes ?* Une question difficile qui, nous le pensons, pourrait faire l'objet d'une réunion à part .

Une dimension particulièrement ambitieuse du PNRR, un programme durement critiqué par nous et à juste titre[29] (Ioan-Franc, Diamescu 2021), se considérant plus nécessaire pour remettre la Roumanie à d'autres objectifs, tels que la cyber-économie, que de revenir au moment/état avant l'action des facteurs perturbateurs. Et voila, l'approche PNRR du sujet confirme notre pensée. La composante 9 – soutien au secteur privé, à la recherche, au développement et à l'innovation – avec une dotation de 1.064 millions d'euros, vise principalement à soutenir la numérisation future des entreprises et à réaliser un projet multinational sur les « *processeurs à faible énergie et les puces à semi-conducteurs* », à mettre en œuvre en tant que Projet d'Intérêt Commun Européen Important (PIIEC). En outre, le PNRR finance l'opérationnalisation d'une plateforme numérique publique, qui fournit aux entreprises des services liés à l'entrée / sortie des entreprises du marché, l'autorisation des représentations étrangères en Roumanie et l'obtention de licences industrielles, ainsi qu'un programme d'une valeur de 500 millions d'euros, visant à soutenir l'adoption de technologies/solutions numériques, telles que l'intelligence artificielle, les données, le cloud computing, les plateformes, la technologie *blockchain* et la transformation digitale des procédures d'entreprise.

29 Ioan-Franc, V.; Diamescu, A.-M., 2021 – *The Crisis after the Crisis – Resilience or Reset ?*, l'Amphithéâtre économique, 58, p. 864, DOI: 10 24818/E1/2021/58/864

Il reste à voir quels seront les objectifs et dans quelle mesure ils seront pleinement atteints, mais les conclusions que nous pouvons formuler à cette date, sans crainte de faire des erreurs, sont, à notre avis, deux :

(1) la voie vers la **cyber-economy** est irréversible, la vitesse à laquelle les États y parviendront dépend de manière déterminante leur niveau de compétitivité ;

(2) **le souci des Etats de réglementer**, au moins d'un point de vue moral, la façon dont les nouvelles technologies (intelligence artificielle, cloud, blockchain, etc.) sont intégrées dans la vie économique et sociale **reste secondaire à la chasse du profit des grandes entreprises dans le domaine**.

En d'autres termes, nos préoccupations restent responsables et nécessaires !

References

Dicu A., Dans un avenir qui ne sera pas du tout « SF ». Les robots nous remplaceront au travail. Les prédictions d'Alexandru Mironov : « Nous ne résisterons pas à l'émancipation de l'intelligence artificielle. », 11.fév., 2023, sur https://www.fanatik.ro/intr-un-viitor-deloc-sf-robotii-ne-vor-inlocui-la-serviciu-predictiile-lui-alexandru-mironov-nu-vom-rezista-in-fata-emanciparii-inteligentei-artificiale-20305403

Dumitrache I, Cyber-phisical-systems (CPS) – un facteur clé dans l'économie du savoir et de l'innovation, dans la Revue Roumaine de l'Informatique et du Contrôle Automatique, vol. 23. No 4, 2013, p. 44 sur http://www.rria.ici.ro

Ioan-Franc, V.; Diamescu, A.-M., 2022 – Richesse versus prospérité partagée – la clé de la moralité et de la responsabilité de développement soutenable, ¿Por qué no un mundo sostenible? La ciencia económica va a su encuentro, Real Academia de Ciencias Económicas y Financieras, Barcelona

Ioan-Franc, V.; Diamescu, A.-M., 2021 – The Crisis after the Crisis – Resilience or Reset ?, l'Amphithéâtre économique, 58, p. 864, DOI: 10 24818/E1/2021/58/864

Ioan-Franc, V.; Diamescu, A.-M., 2023 - L'intelligence artificielle - opportunités, responsabilité, inquiétudes, Synthèse du discours prononcé à la réunion RACEF-BEN avec l'Université de Kragujevac – Serbia, 23 avril 2023

Ionescu, V., Experts: ChatGPT peut mener à des escroqueries sentimentales , 19 Fév. 2023, sur https://cursdeguvernare.ro/experti-chatgpt-poate-duce-la-aparitia-escrocheriilor-sentimentale.html

Ionescu, V., The Guardian: La révolution industrielle menée par l'intelligence artificielle menace les emplois de la classe moyenne, 19 Fév. 2023 sur https://cursdeguvernare.ro/the-guardian-revolutia-industriala-antrenata-de-inteligenta-artificiala-ameninta-locurile-de-munca-ale-clasei-de-mijloc.html

Lowe, A., Dentons sondage IA: principales conclusions, dans Passer au numérique, Déc. 2021 sur https://www.businessgoing.digital/dentons-ai-survey-key-findings/

Radu, C., Roumanie: Un « champion caché » de la numérisation ? Que sait ChatGPT et que savent les spécialistes ? Entretien avec l'Intelligence Artificielle sur la numérisation en Roumanie, 12.02.2023 sur https://economedia.ro/romania-un-campion-ascuns-al-digitalizarii-ce-stie-chatgpt-si-ce-stiu-specialistii-o-conversatie-cu-artificial-intelligence-despre-digitalizarea-in-romania.html#.ZCvktntBy3A

Dentons, Guide de l'Intelligence Artificielle 2022 Le parcours de l'intelligence artificielle – ouvrir les yeux sur les possibilités et les risques , Dec. 2021, sur https://www.acc.com/sites/default/files/resources/upload/Dentons

Commission Européenne, Index de l'Economie Digitale et de la Société (DESI) 2022; chapitres thématiques, pe https://digital-strategy.ec.europa.eu/en/policies/desi

Institut National de Statistique, Communiqué de presse: Premières données provisoires pour le Recensement de la Population et du Logement, étape de 2021, sur https://insse.ro/cms/sites/default/files/com_presa/com_pdf/cp-date-provizorii-rpl2021.pdf

Les chefs d'entreprise mondiaux expriment leurs principales préoccupations concernant l'utilisation de l'Intelligence Artificielle, Jan. 2022, sur https://www.dentons.com/en/about-dentons/news-events-and-awards/news/2022/january/global-business-leaders-voice-major-concerns-over-the-use-of-artificial-intelligence

https://stirileprotv.ro/stiri/ilikeit/rector-umfst-statul-trebuie-sa-impuna-consideratii-morale-in-dezvoltarea-ia-exista-riscul-ca-omul-sa-piarda-controlul.html

https://www.acc.com/sites/default/files/resources/upload/Dentons%20Artificial%20Intelligence%20Guide%202022.pdf

https://www.trade.gov/country-commercial-guides/romania-information-communications-technology-ict

https://www.trade.gov/country-commercial-guides/romania-information-communications-technology-ict

https://www.trade.gov/country-commercial-guides/romania-information-communications-technology-ict

https://www.trade.gov/country-commercial-guides/romania-information-communications-technology-ict

https://www.trade.gov/country-commercial-guides/romania-information-communications-technology-ict

INTERVAL-VALUED INTUITIONISTIC FUZZY MODEL FOR SIMULATION OF AZERBAIJAN NATIONAL CYBER SECURITY INDEX

Dr. Korkmaz Imanov
Académico Correspondiente por Azerbaiyán de la Real Academia de Ciencias Económicas y Financieras

Aliyev A.
Ministry of Science and Education Republic of Azerbaijan

Abstract.
In this paper, we proposed an approach based on interval-valued intuitionistic fuzzy instruments to evaluate National Cyber Security Index (NCSI) that is one of main factors constituting national security. Ǐnterval-valued intuitionistic fuzzy techniques are suitable in this regard to solve this kind of Weighted Linear Combination (WLC) problems and simulate possible increment range in the overall index. Considering the fact that there is not a generalized way for computation of global indices, and Principal Component Analysis (PCA) is the main method, dealing with data uncertainty requires fuzzy logic and its extension-based approaches. The novelty of the current paper is that it takes into account the fuzzyness of crisp input data, and simulation of input data conveys the possible change extent, expressed as inteval-valued intuitionistic fuzzy numbers. The elaborated methodology in the given work can be a piece of help in the generalization of NCSI computating methodology and for the index control purposes.

Keywords: National Cyber Security Index, interval-valued intuitionistic fuzzy MCDM, simulation model.

1. Introduction

Cybersecurity is the management, governance, development, and application of information security, operational technology security, and information technology security hardware and software for obtaining regulatory compliance, protecting assets and to put at risk the assets of challengers [1].

Cybersecurity is not just a technical issue but a complex multi-faceted problem, aspects of which extend beyond social and economic development areas as international relations, trade negotiations, sustainable development, law enforcement, national and international security [2].

After the Cold War political discords entailed cyber-attacks [3], enforcing countries to develop their own cyber security systems. Cybersecurity remains reasonably important at a higher place in present-day business with the sharp and turbulent environment.

The internet has been recently turned into a locale for digital crime, cyber-attack, cyber harassment, and information leakage on a large scale. In the sequence of cyber-attacks on countries: Estonia in 2007, Georgia in 2008, Kyrgyzstan in 2009, South Korean's banks in 2010, Stuxnet malware as Iran case in 2010, Cyber espionage against US in 2012, New York dam's SCADA systems in 2016 or LinkedIn mass data cracking in 2013, Yahoo in 2014, Dropbox in 2014, and Telegram in 2016 have urged almost all national governments to reconsider the cybersecurity risk perspectives, and its potential effects on society, economy, and critical infrastructures.

According to UN report [4] main types of threat actors in the cyberenvironment are:

- Hackers - individuals or groups harming for fame or thrilling.
- Hacktivists - hackers with a specific political or ideological motive.

- Cybercriminals - actors from small outfits to large, organized crime networks who engage in crimes such as fraud, theft, extortion etc.
- Industrial spies – actors with the goal to obtain trade secrets, blackmailing for economic interest reasons, or sabotaging the competition, in the corporate world.
- States or state-sponsored groups - well-resourced actors pursuing complex objectives, employed and financed by governments or military outlets.
- Insiders - actors endangering the entity from within, including disgruntled employees and inadequately trained personnel or contracted service providers.

Participation in the Internet economy cannot be ignored by countries which covers or influences most spheres of socio-economic prosperity. [2] Cybersecurity is affected by a number of factors within the national scope and each country should adopt the following better practices of National Cyber Security Strategy:

√ Governance

√ Risk management in national cybersecurity

√ Preparedness and resilience

√ Security of Critical Infrastructure and essential services

√ Capability and capacity building and awareness raising

√ Legislation and regulation

√ International cooperation

Kolini and Janczewski classified the world organizations dealing with cybersecurity policy and methodology improvement where UN tops the list with 193 countries, while NATO cooperate 33 countries [5].

Despite the fact that cyber security anxieties rooted from military and politic reasons, today the reasons and motives may be numerous and to protect national digital assets from malicious attacks that can destabilize country politically, economically and etc.

Teoh and Mahmood highlight the cyber threats on digital economies and nations. They addressed security and defense issues in this regard [6].

Galinec and et al. classified the cybersecurity as: information security, information technology (IT) security, operational security, and offensive security, also distinguished the terms: cyberwarfare, cyberterrorism, cybercrime, and tried to give the definition of cybersecurity [7].

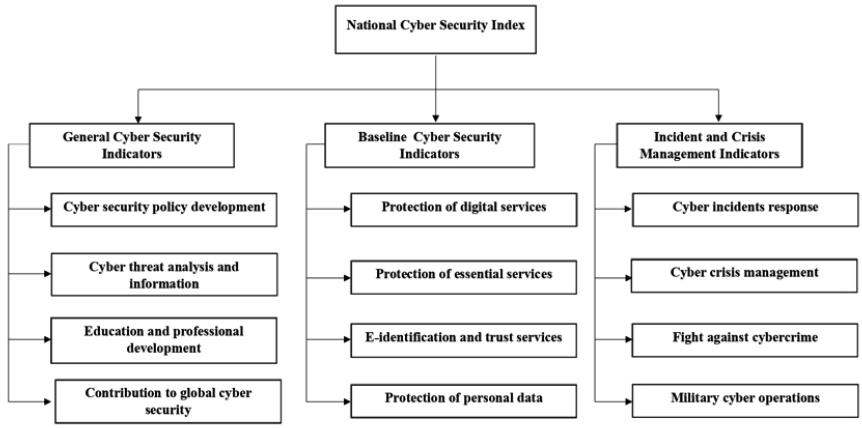
E-learning necessitates a cyber platform to run the business processes, and the platform must be protected for the users to share the data. The paper by Buja and et al. underlines the main cybersecurity features in the National e-Learning policy [8].

The National Cybersecurity Index (NCSI) developed and guided by the e-Governance Academy has since 2016 functioned as a key instrument to support cybersecurity activities and countries on increment of their national cybersecurity capacities.

The NCSI indicators were developed (diagram 1) based on the national cyber security context . The main cyber threats constituting the sub-indices bear the following concepts:

1. Making e-services inaccessible;
2. Breaking the data integrity;
3. Breaking the data confidentiality [9].

Diagram 1. NCSI indicators.



As generalization of intuitionistic fuzzy sets, interval-valued intuitionistic fuzzy sets (IVIFS) are more effective to deal with uncertain information and to take into account ambiguity [10,11]. With the intention to evaluate compound NCSI, interval-valued intuitionistic fuzzy weighted averaging operator (IIFWA) that is developed by Xunjie and et al. [12] will be employed. In solution of the relevant weighted linear combination problems, application of interval-valued intuitionistic fuzzy aggregation operators are uniquely effective given that those can be applied with the aim to combine multiple values into a composite quantity.

The paper is organized as following: paragraph 2 covers statement of the problem. Paragraph 3 introduces the solution algorithm for the problem. In the last paragraph, some extracts from computation, and simulation process for overall NCSI are provided.

2. Statement of the problem

In this paper, the main idea is to present a simulation model based on interval-valued intuitionistic fuzzy techniques for the computation and con-

trol purposes of NCSI. With this intention, a solution algorithm is developed containing interval-valued intuitionistic fuzzy tools. For the fuzzification purposes the NCSI data for 2023 with their (maxima and minima) are acquired from e-Governance Academy Foundation [13] which is provided in table 1.

Table 1. NCSI data on Azerbaijan

Nº	National Cyber Security Index	Acronyms	Data for 2023	Best case	Worst case
1. General Cyber Security Indicators		**GCSI**			
Cyber security policy development		CSPD	2	7	0
Cyber threat analysis and information		CTAI	4	5	0
Education and professional development		EPD	8	9	0
Contribution to global cyber security		CGCS	2	6	0
2. Baseline cyber security indicators		**BCSI**			
Protection of digital services		PDS	0	5	0
Protection of essential services		PES	6	6	0
E-identification and trust services		EITS	7	9	0
Protection of personal data		PPD	1	4	0
3. Incident and crisis management indicators		**ICMI**			
Cyber incidents response		CIR	3	6	0
Cyber crisis management		CCM	1	5	0
Fight against cybercrime		FAC	9	9	0
Military cyber operations		MCO	3	6	0

3. An algorithm for computation of NCSI

The algorithm developed for computation of NCSI is introduced below:

Step 1. Interval-valued intuitionistic fuzzification of crisp data. For the fuzzification purpose interval-valued intuitionistic fuzzification triangular function is applied [14].

$$\mu_A^-(x)=\begin{cases}\mu^-\frac{(x-a)}{(b-a)},\\ \mu^-;\\ \mu^-\frac{(c-x)}{(c-b)};\end{cases}\qquad \mu_A^+(x)=\begin{cases}\mu^+\frac{(x-a)}{(b-a)}, & a<x<b\\ \mu^+; & x=b\\ \mu^+\frac{(c-x)}{(c-b)}; & b<x<c\end{cases} \tag{1}$$

$$v_A^-(x)=\begin{cases}1-(1-v^-)\frac{(x-a)}{(b-a)},\\ v^-;\\ v^-+(1-v^-)\frac{(x-b)}{(c-b)};\end{cases}\qquad v_A^+(x)=\begin{cases}1-(1-v^+)\frac{(x-a)}{(b-a)}, & a<x<b\\ v^+; & x=b\\ v^++(1-v^+)\frac{(x-b)}{(c-b)}; & b<x<c\end{cases} \tag{2}$$

Where, $\mu^- : X \to [0,1]$, and $\mu^+ : X \to [0,1]$ denote the lower and upper membership degrees, $v^- : X \to [0,1]$, and $v^+ : X \to [0,1]$ denote the lower and upper non-membership degrees respectively.

Step 2. Construction of interval-valued intuitionistic fuzzy preference relation matrix (IVIFPRM).

In this stage based on the scale given in table 2, IVIFPRM is established [15].

Table 2. Linguistic terms for criteria preference

Linguistic terms	Acronyms	IVIFNs
Extremely important	EXI	([0.65,0.75],[0.10,0.25])
Very Important	VI	([0.60,0.70],[0.15,0.30])
Important	I	([0.55,0.65],[0.20,0.35])
Medium Important	MI	([0.50,0.60],[0.25,0.40])
Equally important	EI	([0.50,0.50],[0.50,0.50])
Medium Low Important	MLI	([0.45,0.55],[0.30,0.45])
Low Important	LI	([0.25,0.40],[0.50,0.60])

Employing the interval-valued linguistic fuzzy value counterparts of linguistic terms for criteria preference the IVIFPRM is set up for each sub-index of NCSI.

$$R = \begin{array}{c} \\ C_1 \\ C_2 \\ \vdots \\ C_m \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \cdots & C_n \end{array} \\ \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{m1} & r_{m2} & \cdots & r_{mn} \end{pmatrix} \end{array}$$

Step 3. Checking the additive consistency. If $R = (r_{ij})_{n\times n} \subset X \times X$, where $r_{ij} = [\underline{r}_{ij}, \bar{r}_{ij}]$ stands for the preference degree interval of alternative x_i over x_j. Then the following conditions must hold [16] for $\underline{r}_{ij}$ and $\bar{r}_{ij}$:

$$0 \le \underline{r}_{ij} \le \bar{r}_{ij} \le 1,\ \underline{r}_{ij} + \bar{r}_{ij} = 1,\ \underline{r}_{ij} = \bar{r}_{ij} = 0.5 \text{ for all } i, j = 1,2,...,n \tag{3}$$

Step 4. Checking the multiplicative consistency. For the multiplicative consistent interval-valued intuitionistic fuzzy preference relation $\widetilde{R}$, the following equations [17] must hold:

$$\tilde{\mu}_{ij}^{L} = \frac{\sqrt[j-i-1]{\prod_{k=i+1}^{j-1} \tilde{\mu}_{ik}^{L}\tilde{\mu}_{kj}^{L}}}{\sqrt[j-i-1]{\prod_{k=i+1}^{j-1} \tilde{\mu}_{ik}^{L}\tilde{\mu}_{kj}^{L}} + \sqrt[j-i-1]{\prod_{k=i+1}^{j-1}(1-\tilde{\mu}_{ik}^{L})(1-\tilde{\mu}_{kj}^{L})}}, j > i+1 \tag{4}$$

$$\tilde{\mu}_{ij}^{U} = \frac{\sqrt[j-i-1]{\prod_{k=i+1}^{j-1} \tilde{\mu}_{ik}^{U}\tilde{\mu}_{kj}^{U}}}{\sqrt[j-i-1]{\prod_{k=i+1}^{j-1} \tilde{\mu}_{ik}^{U}\tilde{\mu}_{kj}^{U}} + \sqrt[j-i-1]{\prod_{k=i+1}^{j-1}(1-\tilde{\mu}_{ik}^{U})(1-\tilde{\mu}_{kj}^{U})}}, j > i+1 \tag{5}$$

$$\tilde{v}_{ij}^{L} = \frac{\sqrt[j-i-1]{\prod_{k=i+1}^{j-1} \tilde{v}_{ik}^{L}\tilde{v}_{kj}^{L}}}{\sqrt[j-i-1]{\prod_{k=i+1}^{j-1} \tilde{v}_{ik}^{L}\tilde{v}_{kj}^{L}} + \sqrt[j-i-1]{\prod_{k=i+1}^{j-1}(1-v_{ik}^{L})(1-\tilde{v}_{kj}^{L})}}, j > i+1 \tag{6}$$

$$\tilde{v}_{ij}^{L} = \frac{\sqrt[j-i-1]{\prod_{k=i+1}^{j-1} \tilde{v}_{ik}^{L}\tilde{v}_{kj}^{L}}}{\sqrt[j-i-1]{\prod_{k=i+1}^{j-1} \tilde{v}_{ik}^{L}\tilde{v}_{kj}^{L}} + \sqrt[j-i-1]{\prod_{k=i+1}^{j-1}(1-v_{ik}^{L})(1-\tilde{v}_{kj}^{L})}}, j > i+1 \tag{7}$$

Step 5. Calculation of Entropy. Entropy measures are computed employing the approach established by Yager [18,19] that is given below:

$$E_Y(A) = \frac{1}{n}\sum \frac{2 - |\mu_A^L(x_i) + \mu_A^U(x_i) - v_A^L(x_i) - v_A^U(x_i)| + \pi_A^L(x_i) + \pi_A^U(x_i)}{2 + |\mu_A^L(x_i) + \mu_A^U(x_i) - v_A^L(x_i) - v_A^U(x_i)| + \pi_A^L(x_i) + \pi_A^U(x_i)} \tag{8}$$

Step 6. Construction of Entropy matrix. Employing formula (8) entropy matrix $E = (e_{ij})_{m\times n}$ is constructed:

$$E = \begin{array}{c} \\ C_1 \\ C_2 \\ \vdots \\ C_m \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \cdots & C_n \end{array} \\ \begin{pmatrix} e_{11} & e_{12} & \cdots & e_{1n} \\ e_{21} & e_{22} & \cdots & e_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ e_{m1} & e_{m2} & \cdots & e_{mn} \end{pmatrix} \end{array}$$

Step 7. Obtaining the criteria weights. Initially the entropy information measure is computed [20,21] with the following formula:

$$E_j = \frac{1}{m}\sum_{i=1}^{m} e_{ij} \tag{9}$$

Then, the criteria weights are computed [20,21] with the following equation:

$$w_j = \frac{1 - E_j}{\sum_{j=1}^{n}(1 - E_j)} \tag{10}$$

Step 8. In this stage, interval-valued intuitionistic fuzzy weighted aggregation operator (IIFWA) is applied in order to combine interval-valued intuitionistic fuzzy values for NCSI indicators [11]:

$$IIFWA_w(\tilde{\alpha}_1, \tilde{\alpha}_2, \ldots, \tilde{\alpha}_m) = \left(\left[1 - \prod_{i=1}^{m} (1 - a_i)^{w_i}, 1 - \sum_{i=1}^{m} (1 - b_i)^{w_i} \right], \left[\prod_{i=1}^{m} {c_i}^{w_i}, \prod_{i=1}^{m} {d_i}^{w_i}, \right] \right) \tag{11}$$

Step 9. In the final step, obtained interval-valued intuitionistic fuzzy values are interpreted by linguistic terms to get comprehensible results [22]. The linguistic terms set with their interval-valued intuitionistic fuzzy values are given in table 3.

Table 3. Linguistic terms and their matching interval-valued intuitionistic fuzzy scale

Linguistic terms (*LT*)	IFNs membership and non-membership function value intervals
	$([\mu^-, \mu^+], [v^-, v^+]$
Very high (VH)	([1.00, 1.00], [0.00, 0.00])
High (H)	([0.70, 0.80], [0.05, 0.10])
Medium high (MH)	([0.60, 0.70], [0.15, 0.20])
Medium (M)	([0.50, 0.60], [0.25, 0.30])
Medium low (ML)	([0.30, 0.40], [0.45, 0.50])
Low (L)	([0.15, 0.25], [0.55, 0.60])
Very low (VL)	([0.00, 0.10], [0.85, 0.90])

Step 10. Simulation. The initial result is obtained employing the actual data. Then different scenarios are considered with the purpose to control the NCSI index within the country level.

4. Computation and simulation results of NCSI

In this section, as an example, computation part for General Cyber Security Indicators is provided. Actual data converted into interval-valued intuitionistic fuzzy numbers are given in table 4.

Table 4. Data as interval-valued intuitionistic fuzzy numbers

Nº	Acronims	Actual Data	Interval-valued intuitionistic fuzzy numbers
1.	**GCSI**		
1.1	CSPD	2	[0.26,0.27],[0.71,0.72]
1.2	CTAI	4	[0.72,0.76],[0.21,0.22]
1.3	EPD	8	[0.8,0.84],[0.12,0.13]
1.4	CGCS	2	[0.30,0.32],[0.67,0.68]
2.	**BCSI**		
2.1	PDS	0	[0,0],[1,1]
2.2	PES	6	[0.90,0.95],[0.01,0.03]
2.3	EITS	7	[0.70,0.74],[0.23,0.24]
2.4	PPD	1	[0.23,0.24],[0.75,0.77]
3.	**ICMI**		
3.1	CIR	3	[0.45,0.48],[0.51,0.52]
3.2	CCM	1	[0.18,0.19],[0.80,0.81]
3.3	FAC	9	[0.90,0.95],[0.01,0.03]
3.4	MCO	3	[0.45,0.48],[0.50,0.51]

Following the conversion of crisp data into interval-valued intuitionistic fuzzy values, referring to steps 2 to 4, IVIFPR and consistent IVIFPR matrices are constructed as below:

$$R = \begin{array}{c} \\ \text{CSPD} \\ \text{CTAI} \\ \text{EPD} \\ \text{CGCS} \end{array} \begin{pmatrix} \textit{CSPD} & \text{CTAI} & \text{EPD} & \text{CGCS} \\ ([0.50,0.50],[0.50,0.50]) & ([0.50,0.60][0.25,0.40]) & ([0.55,0.65],[0.20,0.35]) & ([0.60,0.70],[0.15,0.30]) \\ ([0.25,0.40],[0.50,0.60]) & ([0.50,0.50],[0.50,0.50]) & ([0.50,0.60][0.25,0.40]) & ([0.55,0.65],[0.20,0.35]) \\ ([0.20,0.35],[0.55,0.65]) & ([0.25,0.40],[0.50,0.60]) & ([0.50,0.50],[0.50,0.50]) & ([0.50,0.60][0.25,0.40]) \\ ([0.15,0.30],[0.60,0.70]) & ([0.20,0.35],[0.55,0.65]) & ([0.25,0.40],[0.50,0.60]) & ([0.50,0.50],[0.50,0.50]) \end{pmatrix}$$

$$\tilde{R} = \begin{array}{c} \\ \text{CSPD} \\ \text{CTAI} \\ \text{EPD} \\ \text{CGCS} \end{array} \begin{pmatrix} \text{CSPD} & \text{CTAI} & \text{EPD} & \text{CGCS} \\ ([0.50,0.50],[0.50,0.50]) & ([0.50,0.60][0.25,0.40]) & ([0.50,0.69],[0.10,0.31]) & ([0.55,0.74],[0.08,0.26]) \\ ([0.25,0.40],[0.50,0.60]) & ([0.50,0.50],[0.50,0.50]) & ([0.50,0.60][0.25,0.40]) & ([0.50,0.69],[0.10,0.31]) \\ ([0.10,0.31],[0.50,0.69]) & ([0.25,0.40],[0.50,0.60]) & ([0.50,0.50],[0.50,0.50]) & ([0.50,0.60][0.25,0.40]) \\ ([0.08,0.26],[0.55,0.74]) & ([0.10,0.31],[0.50,0.69]) & ([0.25,0.40],[0.50,0.60]) & ([0.50,0.50],[0.50,0.50]) \end{pmatrix}$$

In the next step, observing the steps 5 and 6, elements of entropy matrix are assessed:

$$E = \begin{array}{c} \\ CSPD \\ CTAI \\ EPD \\ CGCS \end{array} \begin{array}{c} \begin{array}{cccc} CSPD & CTAI & EPD & CGCS \end{array} \\ \begin{pmatrix} 1 & 0.8 & 0.7143 & 0.6690 \\ 0.8 & 1 & 0.8 & 0.7143 \\ 0.7143 & 0.8 & 1 & 0.8 \\ 0.6690 & 0.7143 & 0.8 & 1 \end{pmatrix} \end{array}$$

Following the construction of entropy matrix, the criteria weights are calculated according to equations given in step 7:

$$E_1 = 0.7973, \quad E_2 = 0.8327, \quad E_3 = 0.8286, \quad E_4 = 0.7973$$

$$w_1 = 0.2718, \quad w_2 = 0.2282, \quad w_3 = 0.2282, \quad w_4 = 0.2718$$

Consequently, interval-valued intuitionistic fuzzy weighted aggregation operator is computed as an example for the General Cyber Security Indicators then in a similar way for the overall NCSI.

$$IIFWA_{GCSI} = (1 - [((1-0.26)^{0.2718} * (1-0.72)^{0.2282} * (1-0.8)^{0.2282} * (1-0.3)^{0.2718}), ((1-0.27)^{0.2718} * (1-0.76)^{0.2282} * (1-0.84)^{0.2282} * (1-0.32)^{0.2718})], [(0.72^{0.2718} * 0.21^{0.2282} * 0.12^{0.2282} * 0.67^{0.2718}), (0.72^{0.2718} * 0.22^{0.2282} * 0.13^{0.2282} * 0.68^{0.2718})] = ([0.57,0.61], [0.35,0.37])$$

Following the computation algorithm for all subindices, the NCSI is aggregated:

$$IIFWA_{NCSI} = ([0.58,0.64],[0.27,0.31])$$

In due course, for the simulation purpose five scenarios are put forward for the assessment of high level of NCSI. The possible increment of five lower indicators: Cyber security policy development, Contribution to global cyber security, Protection of digital services, Protection of personal data, and Cyber crisis management are taken into account. The obtained results shown in table 5 indicates that a unit change in PDS and PPD strengthens NCSI from me-

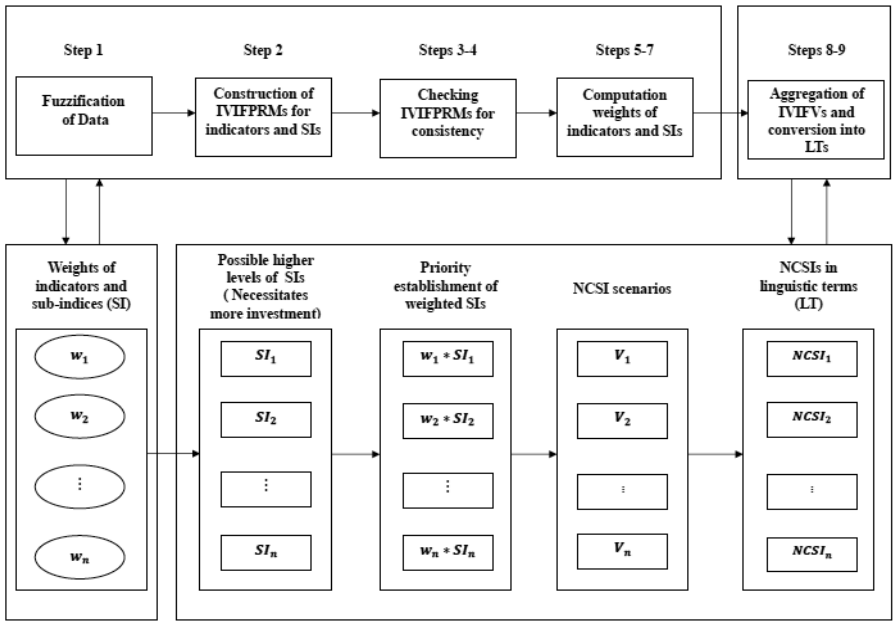
dium to medium high, and two units change in PDS along with a unit increment in the indicators CSPD, CGCS, and CCM might improve NCSI index to the high level.

Table 5. Simulation results

№	Acronims	Actual Data	V1	V2	V3	V4	V5
1.	**GCSI**						
1.1	CSPD	2	2	2	3	3	4
1.2	CTAI	4	4	4	4	4	4
1.3	EPD	8	8	8	8	8	8
1.4	CGCS	2	2	2	2	2	3
2.	**BCSI**						
2.1	PDS	0	1	1	2	2	3
2.2	PES	6	6	6	6	6	6
2.3	EITS	7	7	7	7	7	7
2.4	PPD	1	1	2	2	2	3
3.	**ICMI**						
3.1	CIR	3	3	3	3	3	3
3.2	CCM	1	1	1	1	2	3
3.3	FAC	9	9	9	9	9	9
3.4	MCO	3	3	3	3	3	3
IVIFVs		[0.58,0.64], [0.27,0.31]	[0.59,0.65], [0.26,0.31]	[0.60,0.66], [0.26,0.30]	[0.61,0.67], [0.24,0.29]	[0.62,0.68], [0.24,0.28]	[0.67,0.73], [0.21,0.24]
LT		M	MH	MH	MH	MH	H

Despite the fact that linguistic terms are more helpful to understand the change in overall index, interval-valued intuitionistic fuzzy numbers are more advantageous to track the dynamics of general index within the simulation process. The simulation process is provided in diagram 2.

Diagram 2. NCSI simulation and control process



Conclusion

In this paper, the NCSI is computed with IIFWA operator taking into account weights of sub-indices and indicators. Obtained results over actual data reflect NCSI level in the country and outcomes over simulated scenarios can be used for the improvement of the NCSI index over the certain indicators. In the last section NCSI outputs as an aggregated interval-valued intuitionistic fuzzy values are converted into linguistic terms for clear understanding. But, the computation of priority weights of indicators and sub-indices affecting the actual overall index is a different research direction. The difference of current approach from our earlier analogous methods in computation of global indices is the application of fuzzy logic based-extension instruments. The proposed approach can be applicable in computation and simulation of other socio-economic indices.

References

1.Walls, Perkins E, Weiss J. Definition: “Cybersecurity”, G00252816. Gartner Inc., 2013.

2.Strategic Engagement in Cybersecurity. Guide to Developing a National Cybersecurity Strategy. International Telecommunication Union (ITU), Place des Nations, 1211, Geneva 20, Switzerland, 2nd Edition 2021.

3.B. Daricili, S. Çelik. National Security 2.0: The Cyber Security of Critical Infrastructure. Perceptions, 2021, 26(2), pp. 259-276.

4.Cybersecurity in the United Nations system organizations. Report of the Joint Inspection Unit Prepared by Jorge Flores Callejas, Aicha Afifi and Nikolay Lozinskiy. United Nations, Geneva, JIU/REP/2021/3.

5.F. Kolini, L. Janczewski. Clustering and Topic Modelling: A New Approach for Analysis of National Cyber security Strategies. Pacific Asia Conference on Information Systems 2017 Proceedings. 126.

6.C.S. Teoh, A.K. Mahmood. National cyber security strategies for digital economy. Journal of Theoretical and Applied Information Technology, 2017, 9(13), pp. 6510-6522.

7.D. Galinec, D. Možnik, B. Guberina. Cybersecurity and cyber defense: national level strategic approach. Automatika, 2017, 58:3, pp.273-286, DOI: 10.1080/00051144.2017.1407022.

8.A.G. Buja, N.A Deraman, S.D.M. Wahid, M.A. M. Isa. Cyber Security Features for National E-Learning Policy. Turkish Journal of Computer and Mathematics Education, 2021, 12(5), pp. 1729-1735.

9.https://ega.ee/publication/updating-national-cyber-resilience/

10. K.T. Atanassov, “Intuitionistic Fuzzy Sets”, Fuzzy Sets and Systems, 20, 87-96, 1986.

11. K.T. Atanassov, G. Gargov. Interval valued interval-valued intuitionistic fuzzy sets. Fuzzy Sets and Systems, 31(3), 343–349, 1989.

12. G. Xunjie, L. Huchang, Z.S. Xu. Exponential operations of interval-valued intuitionistic fuzzy numbers. Int. J. Mach. Learn. & Cyber. 2015, Doi 10.1007/s13042-015-0434-6.

13. E-governance Academy Foundation. (2020). National Cyber Security Index. Retrieved from NCSI: https://ncsi.ega.ee/country/az/.

14. S.K. Bharati. Transportation problem with interval-valued intuitionistic fuzzy sets: impact of a new ranking. Progress in Artificial Intelligence 10:129–145, 2021. https://doi.org/10.1007/s13748-020-00228-w.

15. Oztaysi, S.C. Onar, K. Goztepe, C. Kahraman. Evaluation of Research Proposals for Grant Funding Using Interval-Valued Intuitionistic Fuzzy Sets. Soft Computing, 2017, 21, 1203–1218, doi:10.1007/s00500-015- 1853-8.

16. H. Zhuang. Additively Consistent Interval-Valued Intuitionistic Fuzzy Preference Relations and Their Application to Group Decision Making. Information, 2018, 9, 260; Doi:10.3390/info9100260.

17. H. Liao, Z. Xu, M. Xia. Multiplicative consistency of interval-valued intuitionistic fuzzy preference relation. Journal of Intelligent & Fuzzy Systems 27 (2014) 2969–2985 Doi:10.3233/IFS-141256.

18. Yager, R.R. (2004). OWA aggregation over a continuous interval argument with applications to decision making. IEEE Transactions on Systems, Man, and Cybernetics, 34(5), 1952–1963.

19. N. Zhao, Z.S. Xu. Entropy measures for interval-valued intuitionistic fuzzy information from a comparative perspective and their application to decision making. Informatica, Vilnius University, Vol. 27(1), 203–228 203, 2016, Doi: http://dx.doi.org/10.15388/Informatica.2016.82.

20. X.W. Qi, C.Y. Liang, E.Q. Zhang, Y. Ding. Approach to interval-valued intuitionistic fuzzy multiple attributes group decision-making based on maximum entropy. Systems Engineering-Theory and Practice, 2011, 31(10): 1940-1948.

21. M. Sun, J. Liu. A family of entropies on interval-valued intuitionistic fuzzy sets and their applications in multiple attribute decision-making. World Aca-

demy of Science, Engineering and Technology International Journal of Mathematical and Computational Sciences, 7(4), 2013.

22. L. Abdullah, C. Goha, N. Zamrib, M. Othman. Application of interval valued intuitionistic fuzzy TOPSIS for flood management. Journal of Intelligent & Fuzzy Systems 38 (2020) 873–881 Doi:10.3233/JIFS-179455.

UN MOMENTO PARA LA MEMORIA DE EUGEN SIMION

Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras

El 14 del pasado mes de marzo de 2023, nuestra Real Corporación recibió la noticia de que la Academia Rumana, la Fundación Nacional para la Ciencia y el Arte y el Museo Nacional de la Literatura Rumana organizaban los día 25 y 26 de mayo el **Simposium Eugen Simion 90** en memoria de quien fue Presidente de la Academia Rumana y miembro de la red internacional **Barcelona Economics Network**.

Hasta aquí la nota escueta de la convocatoria.

Pero, quienes tuvimos el honor y el placer de compartir jornadas inolvidables con esa extraordinaria personalidad de la cultura europea, sabemos que detrás de estos títulos, se hallaba un humano adornado de todos los atributos que lo convertían en un personaje con un lugar en la Historia.

Creo que, tanto personalmente como de manera institucional, dispongo de la autoridad que me confieren las horas, días y años de trabajo en común, para llevar a buen fin el gran proyecto, ideado por él y la Académica Excma. Dra. Maya Simionescu, que tanta fama y gloria alcanzó, conocido como **Penser l'Europe**.

Rumanía, por aquel entonces, no estaba en lo que era la Unión Europea. Es más, parecía un sueño de mentes excesivamente imaginativas pensar que pudiera llegar a convertirse en realidad.

Eugen Simion y Maya Simionescu lograron reunir un selecto grupo de intelectuales europeos con objeto de crear un ambiente propicio a la incor-

poración a la nueva Europea, a través de un seminario anual que en el otoño rumano se reuniría en su país, aportando sus trabajos en relación a los más importantes retos que el proceso de la integración con Europa iba planteando.

Y Rumanía es hoy Europa, modelo para no pocos países, sobre todo de su entorno geográfico.

¿Es esto todo? No, en absoluto. Solo es para un país como el suyo, situado en el otro extremo de la latinidad, una minúscula parte de lo que ha significado Eugen Simion en la historia de la construcción de la Unión Europea.

Hoy, ahora, se le rinde un merecido homenaje en Bucarest y, con todo nuestro pesar, no hemos podido participar presencialmente en él. Pero no ha existido impedimento alguno para que desde el otro extremo de la latinidad, Barcelona le rinda, también, la más sentida muestra de reconocimiento, con el cariño de ayer, de hoy y de todos los tiempos.

Eugen Simion: maestro, amigo, hombre de bien, tu recuerdo quedará siempre en nuestra memoria.

Eugen Simion descansa en paz.

GUIDELINES FOR THE DEVELOPMENT OF CYBERSECURITY ECONOMICSN

Domenico Marino
Miembro de la Barcelona Economics Network de la Real Academia de Ciencias Económicas y Financieras

Pietro Stilo
Mediterranea University of Reggio Calabria

Davide Maniscalco
Mediterranea University of Reggio Calabria

Cybersecurity and Economics

The digital revolution that we have been going through for at least two decades now has entailed and is entailing a whole series of changes leading up to the digital transition, which during the pandemic phase of Covid-19, but also after it, has experienced and is experiencing a strong acceleration. All these changes have entailed a transfer from the real world to the virtual world of a whole series of data and information that make their way around the world on a daily basis via the network. These data and information now constitute the vast majority (not to say almost all) of those used and disseminated worldwide. It is tautological that this mass of data and information must be protected and safeguarded, hence other sectors have developed, such as cybersecurity, and within it various facets have been identified, going so far as to activate insurance policies on cyber risks, something that was unthinkable a few years ago. Among them in recent times, there has been increasing talk of an aspect that is perhaps little known to the general public, but of extreme importance for the years to come, namely cybersecurity economics, or the economics of information security. This is a field of study that focuses on the application of economic principles to cybersecurity, as it has been realized that cybersecurity generates costs but also value, as it protects the most important commodity of our time, or at least one of the most pivotal, namely information and data.

Considering that cyber security has become a key concern for organizations in every sector, economic analysis can provide a useful framework for making informed decisions on risk management and resource allocation.

When we speak of economics applied to the domains of information security, we are therefore referring to a vast field of research that moves from a socio-technical and technological perspective to investigate the following economic aspects of information security

- budget
- information asymmetry
- governance
- types of goods and services

This investigation is, in turn, aimed at a very specific purpose, namely, to identify new sustainable policies, regulatory options and best practices that can improve the cybersecurity posture of players in the digital ecosystem.

In this regard, it should be pointed out from the outset that the economics of cyber security should be understood as an interdisciplinary field of study made functional to cyber security and economics.

Authoritative doctrine (1) has attributed to the economics of cybersecurity the connotation of transdisciplinary (i.e., a synthetic creation that incorporates works from different disciplines), which treats cybersecurity and economics as two different, relatively independent systems of thought that interact in a complex socio-technical system.

And it is precisely the characteristic interaction between the two disciplines that allows one to appreciate the level of contamination of one over the other.

The study of the economics of cyber security enables decision makers to make informed and informed decisions that improve guidance in the assessment and management of complex scenarios, ensuring the sustainability of their governance actions in the digital ecosystem.

Drawing on these insights, cybersecurity practitioners have been able to respond to many complex problems that have emerged in the cybersecurity environment over the past two decades.

The academic field of cybersecurity economics is highly interdisciplinary as it combines key findings and tools from disciplines such as sociology, psychology, law, political science and computer science.

Within the cybersecurity discipline, information security is a term often used interchangeably with information security.

However, it must be said that computer security goes far beyond information security to include the protection of information resources and other assets, including human and cyber-physical systems.

According to this view (2), also supported by the international standard ISO/IEC 27032:2012, in information security, a reference to the human factor usually refers to the human role(s) in the security process.

In information security, however, this factor has an additional dimension, namely humans as potential targets of cyber-attacks or even humans unknowingly participating in a cyber-attack due to lack of awareness.

The European Information Security Agency (ENISA) has clarified that there is no need for a definition of cyber security (3) because it encompasses all practices and standards involving people, processes and technologies within an organization, group or autonomous environments where computers and cyber-physical systems with valuable data are connected to cyberspace.

According to ISO/IEC 27002, an asset is anything of value to an organization

Assets can be classified into different sub-types according to their convertibility (current and non-current assets), physical existence (tangible or intangible assets) and use (operational or non-operational assets).

With the rapid development of information technology, digital assets have been recognized as critical parts of organizations.

However, information security is not limited to digital assets. Over the past decade, the increasing number of cyber-attacks against physical assets and critical infrastructure (i.e. ex plurimus Stuxnet) has indicated that cyber security can be labelled as a serious cyber and physical challenge for organizations and governments.

For these reasons, an accurate assessment of resources and assets is crucial to make efficient investments in their protection, capital budgets and strategic planning.

Much of the published research on the economics of cybersecurity has focused on the economic evaluation of assets and finding the optimal level of security investment in organizations to protect those assets.

However, the economics of cybersecurity is not only concerned with whether an organization is spending enough to protect its resources and whether the security budget is being spent on the right security measures and controls, but is also concerned with how a digital ecosystem and its operational agents function and behave.

The economics of cyber security covers regulatory changes and competitive pressures (e.g. how cyber security can be aligned with broader business processes).

It studies how the allocation of resources by governments and businesses meets the requirements of creating a resilient cyber environment for themselves and other agents.

Furthermore, the economics of cyber security focuses on the efficiency surrounding decisions made as a result of incentives and policies designed to maximize profit and trust within the environment.

The cyber ecosystem

Among the various topics that cybersecurity economics has triggered almost as an appendix to it, but instead as a pivotal part, is that of the cyber ecosystem, within which all stakeholders in this aspect fall, including the industries in the cyber risk value chain, the risk owners, e.g. companies, but not only them, also individuals and the public sector, companies dealing with cybersecurity, and the insurance sector . But let us go in order.

In general, the cyber risk holders are private companies, individuals and the public sector. According to some scholars, companies also generate value through the use of information and communication technologies (ICT) for their business activities, but in the course of these activities, they may be subject to cyber-attacks. This is why they must be protected and safeguarded.

Both the specialized literature on cyber risk quantification and the cyber risk value chain focus almost exclusively on the public and corporate sectors, leaving out private individuals, whose data and information are important in some cases even beyond the individual (for whom they are always of primary importance). Private individuals are therefore increasingly targeted by cyber-attacks, as they are easier ‘prey’ to attack in many cases, either due to a lack of knowledge of the problem or due to the use of simple forms of cyber protection. Individuals are the target of: identity theft, sensitive information such as credit card numbers and social security .

According to data provided by the International Data Corporation (2019), global ICT investments amount to approximately USD 4.9 trillion in 2020, with an estimated annual growth rate of around 5% until 2023. Increasing digitisation has added value to companies and service and product providers in the area of communication and information technology. This is why many companies have taken out IT insurance to cover against IT risks. In this context, providers of IT protection services can also insure themselves against these risks through an Errors and Omissions (E&O) policy. In this context, the most common errors are in software or temporary interruptions in their cloud protection provision, which obviously represent an IT risk for their customers and a source of liability or fines against them.

The cyber insurance market has gained a lot of momentum since the mid-2010s and has grown by 30 per cent annually, to reach around USD 6 billion in gross premiums in 2020. For up-to-date data, please visit our Market Statistics.

In the field of private insurance, cyber is a very popular and fast-growing area. It is an area that by its very nature is very risky and often difficult to explore by definition. One of the most widespread fears is that of a far-reaching systemic event, just as the same insurers that provide such products are concerned about little-known events, perhaps single ones, but which repeatedly pose a widespread risk. A veritable market for insurance companies and their services has been built around this business, with very strong competition between insurance companies.

The capital market is directly exposed to cyber risks through shares and bonds. While a cyber incident could cause the shares of a single company to plummet, as in the case of Marriot in 2018, where the share value fell by 7% when the breach was announced (see Hermeneut (2018)), a cyber catastrophe could bring down an entire industry sector and even the entire world economy. An analysis of such catastrophic scenarios can be found under 1.2.2 in the cyber-economics.com library. The ILS market as of 2020 (year of the covid-19 pandemic) has become very large (USD 45 billion)(4).

Fundamentals of Cybersecurity Economics

As with any new field of research, the basic starting point is to identify fundamental principles from which an articulated body of knowledge can be built.

The fundamental principles of cybersecurity economics include:

I. Risk management: the main objective of cybersecurity economics is risk management. Organizations need to make decisions on how to invest in cybersecurity by assessing the costs and benefits associated with different risk mitigation strategies. Economic analysis can help identify the most relevant threats and assess the potential financial or reputational losses resulting from security breaches.

II. Resource allocation: Resource allocation is a crucial aspect in cybersecurity economics. Since resources are limited, it is necessary to decide how to allocate them effectively to maximize security. Economic analysis can help determine the optimal mix of investments in security technologies, personnel training, implementation of policies and procedures, and incident response management.

III. Assessment of costs and benefits: cost-benefit analysis is a central element of cybersecurity economics. This involves assessing the costs associated with the implementation of security countermeasures, such as the purchase and maintenance of security solutions, staff training and incident management. At the same time, it is important to estimate the expected benefits of reducing risks, such as preventing financial or reputational losses, maintaining customer confidence and adherence to regulations.

IV. Incentives and disincentives: cybersecurity economics also deals with the incentives and disincentives that influence the cybersecurity behavior of organizations and individuals. For example, the costs of

violations may include fines, legal penalties, loss of customers and reputational damage. The proper design of incentives can promote responsible behavior, such as compliance with security policies and the adoption of preventive measures.

In terms of methods, cybersecurity economics uses several tools and techniques, including:

a. Decision models: the use of mathematical models and optimization algorithms can help evaluate cybersecurity investment decisions. These models can consider factors such as the probability of breaches, the associated costs and the potential benefits of different risk mitigation strategies.

b. Cost-benefit analysis: economic analysis is applied to assess the costs and benefits of cybersecurity decisions. This includes estimating the direct and indirect costs associated with security measures, as well as assessing the expected benefits, such as reduced financial losses, reputation protection and regulatory compliance.

c. Risk assessment: risk assessment is a fundamental method in cybersecurity economics. It consists of identifying and evaluating potential cybersecurity risks, assessing the probability of occurrence of damaging events and the associated financial consequences. These assessments help determine the prioritization of investments and direct resources to the areas of greatest risk.

d. Total Cost of Ownership (TCO) analysis: TCO is a method used to assess the total costs of an IT security infrastructure or solution over its entire lifecycle. This includes not only the initial purchase costs, but also the costs of maintenance, upgrades, staff training and replacement over time. A TCO analysis allows one to assess the efficiency of security solutions and make informed decisions on their implementation.

e. Incentive models: the use of incentive models is one method to promote safe behavior. For example, financial incentives or rewards may be offered for achieving security goals, while disincentives may be introduced for non-compliant behavior or security breaches. These models seek to align the interests of organizations and individuals with cybersecurity goals.

Importantly, cybersecurity economics is an evolving field in which new principles and methods are being developed and applied to address emerging cybersecurity challenges. The ultimate goal is to develop strategies and policies that enable organizations to effectively address cybersecurity threats while protecting their data, reputation and financial interests.

In cybersecurity economics, fuzzy logic can be applied in several areas, including:

1. Risk assessment: risk assessment in cybersecurity often involves a number of factors that are difficult to quantify accurately, such as the probability of a breach or the financial impact. Fuzzy logic can be used to represent and manage the uncertainty associated with these factors, enabling a more flexible and robust risk assessment.
2. Investment decisions: fuzzy logic can be applied to evaluate investment decisions in cyber security, considering trade-offs between costs, benefits and associated uncertainties. For example, it can be used to assess return on investment (ROI) in the presence of partial or uncertain information.
3. Modelling user behavior: fuzzy logic can be used to model user behavior in relation to cyber security. This can provide a better understanding of user preferences and actions and allow security policies to be adapted more effectively.
4. Incident response management: incident response management requires quick and dynamic decisions based on limited and uncertain information. Fuzzy logic can be used to represent and manage uncer-

tainty during incident management, allowing a more flexible evaluation of response options.

The application of fuzzy logic to cybersecurity economics enables the management of uncertainty and imprecision that are inherently present in cybersecurity. This can help to make more realistic decisions by considering a wider range of factors and adapting security strategies in a more flexible and adherent way.

The delineation of a fuzzy logic model

Let X, Y and Z be the linguistic variables representing 'system vulnerability', 'probability of attack' and 'financial impact' respectively. Each of these variables can take linguistic values such as 'low', 'medium' and 'high'.

Definition of linguistic variables:

X = {low, medium, high} Y = {low, medium, high} Z = {low, medium, high}

Definition of membership functions:

For each linguistic variable, we need to define membership functions that assign a degree of membership to each linguistic value. For example, we can use triangular functions to simplify the example:

X_low(x) = triangular(x, 0, 10, 20) X_medium(x) = triangular(x, 15, 25, 35) X_high(x) = triangular(x, 30, 40, 50)

Y_low(y) = triangular(y, 0, 0.2, 0.4) Y_medium(y) = triangular(y, 0.3, 0.5, 0.7) Y_high(y) = triangular(y, 0.6, 0.8, 1)

Z_low(z) = triangular(z, 0, 100, 200) Z_medium(z) = triangular(z, 150, 250, 350) Z_high(z) = triangular(z, 300, 400, 500)

Definition of fuzzy rules:

Fuzzy rules determine how to combine linguistic variables to obtain the desired output. For example:

- If X is high AND Y is high, then Z is high.
- If X is medium AND Y is medium, then Z is medium.
- If X is low AND Y is low, then Z is low.

Fuzzy Inference:

Using the defined fuzzy rules, we can apply fuzzy inference to obtain fuzzy output based on the valuations of linguistic variables. For example, if we have values of X = 25 and Y = 0.5, we can calculate the fuzzy output Z using the defined fuzzy rules and membership functions.

Defuzzyification:

To obtain a numerical value representing the level of risk, we can apply defuzzyfication to the fuzzy output obtained. This involves transforming the fuzzy output into a numerical value representing the overall risk level.

This example illustrates how fuzzy formulae can be used to assess risk in cybersecurity economics. However, it is important to note that the specific membership functions, fuzzy rules and inference algorithms may vary depending on the context and needs of the application.

Defuzzification is the process by which a fuzzy output is converted into a numeric value defined within the variability domain of the output. There are several methods of defuzzification, but one of the most common is the center of gravity or centroid method.

In the center-of-gravity method, the fuzzy output is represented as an aggregate membership function indicating the membership distribution within the variability domain. Defuzzification is done by calculating the centroid or center of gravity of this aggregate membership function.

Here is a step-by-step explanation of the center of gravity method for defuzzification:

i. Aggregation of fuzzy output: The fuzzy output is aggregated using the defined fuzzy rules and appropriate fuzzy operators (such as minimum, maximum or other aggregation operators). The aggregated output represents an aggregated membership function that describes the membership distribution within the variability domain of the output.

ii. Calculation of the centroid: The centroid or center of gravity of the aggregate membership function is calculated using the concept of a weighted average.

iii. Calculation of area under the curve: The area under the curve of the aggregate membership function is calculated using the definite integral. This value represents the sum of the areas of the trapezoids formed by the points of intersection of the curve with the x-axis.
Area = ∫[z_min, z_max] A(z) dz
Where z_min and z_max represent the minimum and maximum x-axis values of the aggregate membership function, respectively.

iv. Calculation of the centroid: The centroid or centre of gravity is calculated as the weighted average of the x-axis points, taking the area under the curve as the relative weight. The formula for calculating the centroid is as follows:
Centroid = (1 / Area) * ∫[z_min, z_max] z * A(z) dz

The value of the centroid represents the numerical result of the defuzzification and indicates the overall risk level.

Note that these formulae are specific to the center of gravity method, which is one of the common defuzzification methods. There are also other defuzzification methods, such as the maximum value method or the maximum center method, which can be used according to the specific needs of the cybersecurity economics problem.

Concluding remarks

In the light of what has been stated in this paper, the economics aspect of cybersecurity is certainly an area of great interest and booming. In the years to come, we will certainly see an increase in this area of cybersecurity. That will go hand in hand with cybersecurity in general, because as everyone knows, the digital sector will be increasingly used by all of us, be it individuals, the public sector, or private companies of any size. It follows that necessarily an impressive amount of data and information will be produced, developed and exchanged all over the world and will have to be protected and safeguarded, such protection has an investment cost, just as potential damages have a cost to be addressed and protected also through dedicated and specific insurance products. The hope is that systemic events can be avoided and that such investment costs are increasingly considered a structural investment by all those affected by such events, who also through adequate information and specific training can avoid frequent incidents by reducing damage and costs.

References

1.- Cat, J. L'unità della scienza. Nella Stanford Encyclopedia of Philosophy; Zalta, EN, ed.; Laboratorio di ricerca sulla metafisica, Stanford University: Stanford, CA, USA, 2017.

2.- Von Solms, R.; Van Niekerk, J. Dalla sicurezza delle informazioni alla sicurezza informatica. Calcola. Sicuro. 2013, 38, 97–102.

3.- ISO/IEC27002. Information Technology–Security Techniques–Code of Practice for Information Security Controls, (AS ISO/IEC 27002: 2015); Organizzazione internazionale per la standardizzazione: Ginevra, Svizzera, 2015.

ENSAYO DE UN ALGORITMO PARA LA GESTIÓN DE LA CIBERSEGURIDAD

Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras

ABSTRACT:
El objetivo principal de este trabajo es la elaboración de un algoritmo capaz de determinar numéricamente el grado o nivel de incidencias óptimas en las estructuras de gestión de la ciberseguridad: en la captación de energías, durante su tránsito a los centros de depósito y distribución y en su utilización cibernética final por parte de las familias y de las actividades económicas.
Este algoritmo permitirá determinar, entre todas las opciones de gestión de ciberseguridad, cuales hay que utilizar para hacer óptima la gestión global.
Nos enfrentamos a **un problema de gestión** complejo por la interconexión de incidencias existente en la gestión de la ciberseguridad a lo largo de todo el recorrido de las energías y de la utilización cibernética final.
Como la vida misma, el algoritmo decisional de la ciberseguridad nos ha mostrado todas sus caras. Con él hemos hallado su mejor y el más humano rostro.

PALABRAS CLAVE: algoritmo humanista, ciberseguridad, deuda ecológica, efectos olvidados, energía limpia, escala semántica endecadaria, escala semántica icosienaria, gestión, "Overshoot Day".

La espada de Damocles del Overshoot Day

Las noticias que año tras año van llegando a los centros de investigación avanzada, ocupados en el tratamiento de los medios de lucha contra la

degradación de nuestro planeta, señalan que el "Overshoot Day", es decir, el día de cada año en el que hemos agotado los recursos que el planeta tierra ha generado y generará a lo largo del propio año, sucede y sucederá antes, si no se adoptan, de manera firme, las medidas pertinentes.

No disponemos, todavía, de esta fecha relativa a 2022, pero en el año anterior, 2021, el Overshoot Day tuvo lugar el 29 de julio. Esto nos indica que para no crear deuda ecológica hubiéramos necesitado la generación de recursos naturales de 1,7 planetas como el nuestro. Los datos parciales de los que se disponen en estos momentos para 2022, siguen en el mismo sentido por cuanto auguran una fecha todavia anterior.

Aun cuando no deseamos engrosar las legiones de catastrofistas que encontramos en las redes sociales y medios de comunicación tradicionales, sí deseamos hacer una llamada a la prudencia de nuestras conciencias, sobre un problema que es grave, aunque sus peores consecuencias se sitúen en la lejanía del tiempo.

Y lo hacemos con los pies en el suelo, proponiendo la elaboración de un algoritmo que permita, de una vez por todas, adelantarnos a los problemas, en lugar de intentar resolver las consecuencias de los mismos.

No pretendemos ser tan ilusos de pensar que la pequeña parcela de investigadores a la que pertenecemos, será capaz de crear los instrumentos, técnicas y procedimientos capaces de dar solución a **todas** las causas que llevan a la progresiva "desertización" de nuestro mundo. Pero sí nos atrevemos a pensar que, si somos capaces de dar solución a uno de ellos, por pequeño que sea, se habrá dado un paso adelante: abrir una puerta puede dar entrada a una luz que ilumine lo suficiente para abrir otras puertas.

Empecemos, pues, por fijar la atención en la parcela que tanto nos ocupa e inquieta como es **la ciberseguridad**, y vamos a hacerlo de manera muy esquemática, como procede en un trabajo como este.

Las energías limpias

Realizado este creemos necesario apunte previo, consideramos útil colocar en el escaparate de las ideas que no se deberían olvidar, aquella que a menudo repetimos: **los trabajos de investigación** cuyo objetivo primero es su utilidad para nuestras vidas, deben tener en cuenta la situación geopolítica de los países en los que serán empleados.

Insistimos en ello, por cuanto en demasiadas investigaciones, por demás de alto valor formal, repletos de citas de famosos economistas de otras latitudes, nos plantean "recetas" válidas en ciertos contextos, pero no útiles en el que las deseamos utilizar.

Nos hallamos en estos momentos en España, con un sistema político que me atrevería a calificar de neoliberal; un país mediterráneo y atlántico a la vez; geográficamente es una península, beneficiada por los vientos que soplan en su valles y en sus montes y picos y gratificada por un soleado casi permanente. Sin embargo, nuestro subsuelo no posee, por el momento, minerales apreciados en el ámbito que analizamos.

Proponemos, pues, intensificar nuestros esfuerzos aprovechando lo que disponemos con holgura, en lugar de empeñarnos en seguir los caminos de personajes brillantes que sí pueden ser útiles en países distintos.

Y esto viene a cuento, en este momento, cuando creemos ha llegado la hora de abordar la ciberseguridad del futuro, cuando seamos capaces de utilizar, mayoritariamente, **energías limpias**.

Para hacerlo mayoritariamente asequible, empecemos recordando que se consideran, en general, como energías limpias, aquellas que no dan lugar a un proceso de eliminación de residuos en la obtención de energía, ni durante su obtención ni durante su utilización.

Se acostumbra a considerar como tales: la energía **solar**, la **eólica**, la **hidráulica**, la **geotérmica** (aprovechando el mayor calor natural del interior de la tierra en relación con la superficie) y el **hidrogeno verde** (se obtiene hidrogeno mediante su separación del agua de diversos materiales, utilizando otra energía limpia).

Su característica más destacable, después de su limpieza, es su capacidad de renovación, entendida esta en el sentido de que, habitualmente, su existencia no es finita.

La gestión de la ciberseguridad

Estamos empeñados en la optimización del proceso de tránsito desde un modelo energético basado principalmente en la utilización de materias fósiles hacia otro de energía limpia y renovable.

Como siempre sucede en los grandes proyectos de esta naturaleza, surgen a la vez que interesantes oportunidades, importantes riesgos, que es necesario prever y darles solución antes de que se presenten en la posterior realidad de los hechos. Es en este sentido que deseamos prestar principal atención al caso específico de la **gestión de la ciberseguridad**.

Y nuestro principal interés radica, sobre todo, en la necesidad de estudiar esta transición desde una perspectiva integral, dados los varios criterios a utilizar para optimizar el proceso que debe llevarla a cabo.

Se halla en la conciencia de los investigadores que utilizan en sus trabajos para la incorporación de energías limpias y renovables una red de energías, que existen relaciones entre los gestores de ciberseguridad en la captación de energías que aumentan, como consecuencia de **potenciales ciberataques** de distinta naturaleza,

Así mismo, tienen lugar conexiones entre los gestores de ciberseguridad de la transmisión de energías así como entre los gestores de ciberseguridad de la utilización cibernética por parte de familias y actividades económicas.

Habitualmente la descripción del flujo de incidencias en la gestión de ciberseguridad suele ser presentado de forma reticular, pero cuando deben realizarse operaciones con él, se expresa bajo forma matricial. Así iniciaremos las siguientes tareas, sin descartar su utilización mediante retículos, cuando lo consideremos necesario o conveniente para una mayor claridad expositiva.

Mirar hacia el futuro es la única manera de prevenir los daños del mañana, protegiendo las instalaciones de creación de las energías limpias y los centros que reciben las energías, así como a quienes utilizan la cibernética resultante de ellas.

Conocido es, que los ciberataques a los centros de producción o captación de estas energías ha aumentado considerablemente en los últimos años como lo ha hecho en el suministro de agua, los transportes, las telecomunicaciones, en las grandes empresas y en el sector financiero, sin olvidar las empresas e instituciones cuyo objetivo es la protección contra los ciberataques.

Y, esto es así, como consecuencia de que los ataques cibernéticos no tienen como único objetivo obtener datos e informaciones o un beneficio económico, también tienen lugar aquellos que persigue producir un daño con la mayor repercusión mediática posible.

Es importantísimo el estudio de la vulnerabilidad de las instalaciones a todos los niveles de estos centros de captación de energías limpias, pero también lo es, creemos, la gestión de ciberseguridad de los mismos.

A este respecto se ha hecho y se está haciendo una meritoria labor por parte de instituciones públicas y privadas, a quienes es necesario hacer patente un merecido reconocimiento.

Principios, proposiciones y escalas semánticas

La elaboración de un algoritmo para abordar un planteamiento de esta naturaleza comporta el seguimiento de los elementos configuradores de toda estructura científica.

En nuestro caso, el primero de ellos corresponde a un poderoso principio: el principio de simultaneidad gradual.

Al amparo de este principio, es posible establecer la siguiente proposición inicial:

"Toda actividad cibernética realiza una adecuada gestión de ciberseguridad"

No podemos limitarnos, hoy, a la respuesta binaria si-no, propia de tiempos pretéritos, bajo el "reinado" del principio del tercio excluso (tertium non datur), por cuanto resulta imprescindible, a nuestros efectos, la **matización**. Y esto es posible con el concepto de "grado" o "nivel".

La **solidez** o, si se quiere, la **calidad** o la **idoneid**ad o la **apreciación**, según sea el caso, es susceptible de ser "numerizada" a través de una escala semántica. Nos hemos acostumbrado a la **endecadaria** (del griego antiguo: once) y ahora nos acostumbraremos, también, a la **eikosienaria** (del griego antiguo: veintiuno).

En la primera de ella tomamos los números, que hacemos corresponder con las palabras que representan, del intervalo de confianza [0 ,1].

En la segunda se toman del intervalo [-1, 1].

Las palabras que deben seguir un orden, son escogidas entre las que se acostumbran a utilizar en cada espacio geográfico y en cada periodo temporal.

Solo a título orientativo se podrían adoptar, para la España de hoy, la siguiente escala semántica endecadaria:

0 : Gestión de ciberseguridad nula

0.1: Gestión de ciberseguridad muy deficiente

0.2: Gestión de ciberseguridad deficiente

0.3: Gestión de ciberseguridad muy floja

0.4: Gestión de ciberseguridad floja

0.5: Gestión de ciberseguridad regular

0.6: Gestión de ciberseguridad más bien positiva

0.7: Gestión de ciberseguridad positiva

0.8: Gestión de ciberseguridad buena

0.9: Gestión de ciberseguridad muy buena

1 : Gestión de ciberseguridad excelente

Utilizaremos, por vez primera la escala semántica eikosienaria[1] para representar el avance o el retroceso en la gestión de la ciberseguridad.

-1: Progreso en la gestión de ciberseguridad totalmente negativo

- 0.9: Progreso en la gestión de ciberseguridad extraordinariamente negativo

-0.8: Progreso en la gestión de ciberseguridad muy negativo

-0.7: Progreso en la gestión de ciberseguridad ampliamente negativo

-0.6: Progreso en la gestión de ciberseguridad excesivamente negativo

1 La primera vez que hemos hallado una escala semántica eikosenaria ha sido en el trabajo de Gil Lafuente, J.; Mulles, A.; Solé Moro, M. L.: "Un algoritmo en base a expertones para facilitar la selección de restaurantes según la tipología de clientes de un hotel" Actas del XXXIII AEDEM anual Meeting. Sevilla, 2019. Pág. 1816-1843.

-0.5: Progreso en la gestión de ciberseguridad sensiblemente negativo
-0.4: Progreso en la gestión de ciberseguridad bastante negativo

-0.3: Progreso en la gestión de ciberseguridad relativamente negativo

-0.2: Progreso en la gestión de ciberseguridad más bien negativo

-0.1: Progreso en la gestión de ciberseguridad prácticamente invariable

0: Progreso en la gestión de ciberseguridad sin avance ni retroceso

0.1: Progreso en la gestión de ciberseguridad más bien positivo

0.2: Progreso en la gestión de ciberseguridad relativamente positivo

0.3: Progreso en la gestión de ciberseguridad bastante positivo

0.4: Progreso en la gestión de ciberseguridad sensiblemente positivo

0.5: Progreso en la gestión de ciberseguridad positivo

0.6: Progreso en la gestión de ciberseguridad francamente positivo

0.7: Progreso en la gestión de ciberseguridad muy positivo

0.8: Progreso en la gestión de ciberseguridad ampliamente positivo

0.9: Progreso en la gestión de ciberseguridad extraordinariamente positivo

1: Progreso en la gestión de ciberseguridad totalmente positivo

Reiteramos cuanto estamos insistiendo sobre la construcción de escalas semánticas, en el sentido de su subjetividad y dependencia del lenguaje habitual de la zona geográfica a la que el algoritmo va destinado.

También, desearíamos hacer hincapié en la eventual utilización de dos escalas semánticas.

Los economistas nos hemos acostumbrado a separar el proceso que lleva a la **decisión** y el que conduce al **análisis y/o contro**l.

Pues bien, al elaborar este trabajo nos hemos encontrado con este caso, que puede resultar paradigmático para dar solución a un problema de optimización, con una escala semántica endecadaria, y para ayudar a solucionar un problema de análisis y control, con una escala semántica eikosienaria.

Informaciones de partida del algoritmo

Pasamos, ya, a entrar en la parte central de este trabajo, en el que priorizamos uno de los grandes objetivos que se desean conseguir: **optimizar la gestión de la ciberseguridad global**, para pasar, luego, a la apertura de puertas a un profundo **análisis** sobre la determinación de aquellas gestiones de ciberseguridad que es necesario potenciar, corregir o cambiar para conseguir aumentar el grado o nivel de la gestión de ciberseguridad a lo largo de todo el recorrido que hemos especificado.

En definitiva, nuestro objetivo parte de unas **informaciones iniciales de gestión** previas del conjunto de elementos incidentes que expresaremos mediante $A = \{ a_1,a_2,\ldots,a_i,\ldots, a_n\}$,, del de la gestión de ciberseguridad del conjunto de elementos incididos $B = \{ b_1, b_2, \ldots, b_j, \ldots, b_m\}$; y de las valuaciones de incidencia directa de la gestión de la ciberseguridad de los elementos incidentes *A* con la de los elementos incididos *B,* (a_i, b_j), es decir, (x_i , y_j), i = 1,2,…, n; j = 1,2,..,m, así como las valuaciones correspondientes al grado o nivel de la gestión de ciberseguridad tanto de los elementos incidentes *A*, sobre sí mismos, (a_i , a_i), es decir (x_i , x_i), i = 1,2,…, n; como también la de los incididos *B*, sobre sí mismos, (b_j, b_j) j= 1,2,..,m, es decir (y_j, y_j), j = 1,2,..,m, estas valuaciones, todas, incluidos en [0 ,1]. Con ellas se pretende encontrar en qué elementos del conjunto *A* es necesario potenciar la gestión de ciberseguridad para optimizar la gestión de ciberseguridad **global.**

Para conseguir este objetivo nos vamos a apoyar en un trabajo original de Kaufmann y Gil Aluja, que más tarde dio lugar a la conocida Forgotten Effects

Theory[2], como hemos hecho en otras ocasiones, entre ellas en el trabajo presentado y publicado recientemente con motivo del Congreso Internacional SIGEF 2022[3], así como en el algoritmo creado y utilizado para reducir la deuda ecológica.[4]

Como primera providencia procederemos a presentar las incidencias de la gestión de ciberseguridad directas, es decir, aquellas que representan el "grado" o "nivel" de incidencia de la gestión de ciberseguridad de toda a_i / i = 1,2,…n sobre la de toda b_j / j = 1,2,…,m, sin tener en cuenta otras incidencias que pudieran actuar como intermediarias.

A efectos de una mayor claridad expositiva vamos a representar el **grado o nivel** de **incidencia** de la gestión de toda a_i / i= 1,2,…n sobre toda la de b_j / j= 1,2,…,m, mediante / i= 1,2,…n; j= 1,2,…,m. Reiteramos que toda valuación / i= 1,2,…n; j= 1,2,…,m debe estar incluida en [0, 1].

El conjunto de la relación de valuaciones en [0, 1] de las incidencias directas de la gestión de ciberseguridad de cada una de las energías limpias a_i / i= 1,2,…n sobre b_j / j= 1,2,…,m, gestión de ciberseguridad de cada una de las actividades económicas, puede ser representado por una matriz borrosa $[\underset{\sim}{M}]$, tal como la siguiente:

2 Kaufmann, A. y Gil Aluja, J.: "Modelos para la investigación de efectos olvidados". Ed. Milladoiro. Vigo 1988 (ISBN: 84-404-3657-2).

3 Gil Aluja, J.: "Economic Humanism Self-indiced in the Circular Economy", en la obra colectiva de Rodríguez García, M. de P. y otros. Ed. SIGEF, 2021 .LNNS 384, pág. 1-12, 2022

4 Gil Aluja, J.: "Un caudal óptimo de recursos para la descarbonización" en la obra: "¿Por qué no un mundo sostenible? La ciencia económica va a su encuentro". Varios autores. Ed. SIGEF, Barcelona, 2023 (ISBN: 978-84-09-48026-5), pág. 87-124.

$[\underset{\sim}{M}]$ =

B / A	b_1	b_2		b_m
a_1	(x_1, y_1)	(x_1, y_2)		(x_1, y_m)
a_2	(x_2, y_1)	(x_2, y_2)		(x_2, y_m)
a_n	(x_n, y_1)	(x_n, y_2)		(x_n, y_m)

En donde las valuaciones de la gestión de ciberseguridad de todo par (a_i, b_j), es decir (x_i,y_j), i = 1,2,…n; j = 1,2,…,m, están incluidas en [0,1].

$$\forall(a_i, b_j) \in [\underset{\sim}{M}] :$$

$$(x_i, y_j) \in [0,1]$$

La matriz $[\underset{\sim}{M}]$ expresa, pues, las **incidencias directas** de la gestión de ciberseguridad de todo elemento a_i / i= 1,2,…n, conjunto **de incidentes** del conjunto A, sobre la de todo elemento de b_j / j= 1,2,…,m, conjunto **de incididos** del conjunto *B*.

Pasamos, seguidamente, a expresar formalmente la **autoinducción de incidencias de la gestión de ciberseguridad,** aunque quizás sea pertinente, antes, señalar que se entiende como autoinducción de incidencias aquellas relaciones de incidencia que tienen lugar entre la gestión de ciberseguridad de los elementos del mismo conjunto, es decir, entre los elementos de *A* entre sí y, de la misma manera, de los elementos de *B*, también entre sí, incluyendo las gestiones de ciberseguridad de un elemento consigo mismo.

Se considera, de esta manera, que, dado un referencial A de elementos incidentes sobre los elementos de otro referencial B de incididos, existen también unas incidencias de la gestión de ciberseguridad a_i / i= 1,2,…n,

sobre la de $a_{h,}$ h = 1, 2, …, n, cuyas correspondientes valuaciones $(x_i, x_h) \in [0, 1]$, i, ,h = 1, 2, …, n, forman una matriz borrosa $[\underset{\sim}{A}]$, cuadrada, sin apelar a la habitual restricción de que también sea reflexiva.

Esta es la razón por la cual este algoritmo que presentamos debe considerarse como una variante de los elaborados con base estricta en la citada "Teoría de los efectos olvidados".

En esta teoría, cuando se hace referencia a las incidencias autoinducidas, se expresa específicamente que la inducción de un elemento a_i sobre a_i y también b_j sobre b_j es igual a la unidad con lo cual las matrices de incidencias $[\underset{\sim}{A}]$ y $[\underset{\sim}{B}]$ son reflexivas, lo que impide que el grado o nivel de las incidencias acumuladas posteriores, después de la convolución, sean inferiores a las directas (x_i, y_j) i= 1,2,…n; j = 1,2,…,m.

$[\underset{\sim}{A}] =$

A \ A	a_1	a_2		a_n
a_1	(x_1, x_1)	(x_1, x_2)		(x_1, x_n)
a_2	(x_2, x_1)	(x_2, x_2)		(x_2, x_n)
a_n	(x_n, x_1)	(x_n, x_2)		(x_n, x_n)

en donde las (x_i, y_j), i= 1,2,…,n, reiteramos una vez más, no tienen porque ser iguales a la unidad.

Igualmente, dado un referencial de elementos incididos, *B*, de otro referencial de incidentes, *A*, son a su vez, incidentes de los elementos de su propio conjunto *B*. Por tanto, existen unas incidencias de la gestión de ciberseguridd de las b_j / j = 1,2,…,m, sobre las de b_k / k= 1,2,…,m, y sus valuaciones (y_j, y_k)

$\in [0, 1]$, j,k =1, 2, …, m, forman una matriz borrosa cuadrada pero no necesariamente reflexiva, $[\underset{\sim}{B}]$:

$[\underset{\sim}{B}]$ =

B \ B	b_1	b_2		b_m
b_1	(y_1, y_1)	(y_1, y_2)		(y_1, y_m)
b_2	(y_2, y_1)	(y_2, y_2)		(y_2, y_m)
b_m	(y_m, y_1)	(y_m, y_2)		(y_m, y_m)

en donde las , (y_j, y_j) j = 1, 2, …, m, reiteramos, no tienen que ser iguales a la unidad.

Se puede decir que entre dos conjuntos: uno de elementos primariamente incidentes, A, y otro primariamente incididos, B, existe, además de un flujo de incidencia de la gestión de ciberseguridad de A sobre B, cuyo grado o nivel directo es representado por una matriz borrosa $[\underset{\sim}{M}]$, otros dos flujos de incidencias en la gestión de ciberseguridad de los elementos de A sobre los elementos A, incluyendo las incidencias en la gestión de ciberseguridad de un elementos sobre sí mismo y otros flujos de incidencias desde los elementos de B sobre los elementos de B, incluyendo, también, las incidencias en la gestión de ciberseguridad de un elemento sobre sí mismo.

Las matrices borrosas $[\underset{\sim}{A}]$ y $[\underset{\sim}{B}]$, expresan las **valuaciones de las incidencias autoinducidas**.

Se dispone, así, de una valiosa información contenida en las tres redes de incidencia: la red de incidencias directas y las dos redes de incidencias autoinducidas.

Obtención del grado o nivel total del flujo de incidencias

Hemos llegado a un estadio de nuestro trabajo en el que se dan por conocidos, en la matriz borrosa $[\underset{\sim}{M}]$ el grado o nivel de los flujos de incidencia directa de la gestión de ciberseguridad del conjunto A de incidencias primarias sobre la gestión de ciberseguridad de los elementos del conjunto *B* de incididos también primarias, en el sentido de **incidencias directas,** sin que se tengan en consideración las posibles incidencias a través de elementos que actúan de intermediarios.

Se acepta, para ello, que en la confluencia de flujos de incidencia, el flujo seguirá hacia aquel de los canales siguientes que permita el mayor flujo posible. Como es habitual en nuestros trabajos, para la potencial incorporación de este fenómeno hemos escogido el operador de **convolución max-min**.

Las matrices que expresan el grado o nivel de incidencias autoinducidas $[\underset{\sim}{A}]$ y $[\underset{\sim}{B}]$ son matrices cuadradas, pero no necesariamente reflexivas.

Si llamamos $[\underset{\sim}{M^*}]$ a la matriz que expresa el grado o nivel global de los flujos de incidencia total, se tendrá:

$$[\underset{\sim}{M^*}] = [\underset{\sim}{A}] \circ [\underset{\sim}{M}] \circ [\underset{\sim}{B}]$$

El procedimiento para el tránsito de flujos de la gestión de ciberseguridad por los canales es muy simple. Basta con hallar, en primer lugar, el grado o nivel de los flujos de incidencias cuando los flujos han transitado por los canales de incidencias de los elementos del conjunto A a los de A y de los elementos de A a los de B, con la convolución max-min $[\underset{\sim}{A}] \circ [\underset{\sim}{M}]$ para cada elemento (a_i, b_j), i = 1,2,…n; j = 1,2,…,m, haciendo:

$$\left(x'_i, y'_j\right) = \bigvee_j \left((x_i, x_h) \wedge \left(x_h, y_j\right)\right)$$

i, h= 1,2,…n

j= 1,2,…,m

el resultado $[\underset{\sim}{A}] \circ [\underset{\sim}{M}]$ incluye además de la posible incorporación de las incidencias directas las de las incidencias autoinducidas de los elementos que primariamente ejercen el papel de **incidentes directos** sobre los elementos del conjunto primariamente de **incididos** del conjunto B.

Procede incorporar, ahora, el grado o nivel del flujo de incidencias correspondiente a las autoincidencias inducidas del conjunto B.

Se hará para cada elemento (a_i, b_j), i= 1,2,…n; j= 1,2,…,m:

$$(x_i^*, y_j^*) = \bigvee_j \left(\left(x'_i, y'_j \right) \wedge \quad (y_j, y_k) \right)$$

i= 1,2,…n

j, k = 1,2,…,m:

El resultado $[\underset{\sim}{M^*}] = ([\underset{\sim}{A}] \circ [\underset{\sim}{M}]) \circ [\underset{\sim}{B}]$ comprende la incorporación de los niveles de incidencia directa de la gestión de ciberseguridad y los de incidencia autoinducida, también de la gestión de la ciberseguridad, por parte del conjunto A de elementos primariamente incidentes y del conjunto B de elementos primariamente incididos: el retablo se halla así completo.

$$[\underset{\sim}{M^*}] = [\underset{\sim}{A}] \circ [\underset{\sim}{M}] \circ [\underset{\sim}{B}]$$

Se posee, entonces, un cuadro total de flujos de incidencias en la red, que está formada por todos los flujos posibles, sin error ni omisión, entre los que se encuentran el o los **caminos con flujo óptimo**, si se acepta el criterio decisorio de prudencia, representado, en nuestro caso, repitámoslo una vez más, por el operador de convolución max-min.

Con satisfacción y legítimo orgullo, expresamos el reconocimiento que ha merecido la obra de Kaufmann y Gil Aluja: "Models per a la recerca d'efectes oblidats"[5], publicada en 1988, antecedente más inmediato, en varios aspectos,

5 Kaufmann, A. y Gil Aluja, J.: "Models per a la recerca d'efectes oblidats". Ed. Milladoiro, Vigo, 1988. (ISBN: 84-404-3657-2)

del procedimiento de cálculo que proponemos, del que puede considerarse una variante.

De esta manera se han podido tener en cuenta todas, absolutamente todas, las incidencias de la gestión de la ciberseguridad existentes, sin error ni omisión, tanto las directas como las que fluyen a través de otros cauces.

El resultado debe proporcionar a que fuente de energía se debe intensificar la gestión para que cada actividad económica consiga su más alto nivel de gestión de la ciberseguridad la que debe rectificarse, modificar o cambiar. Y ello, para todas las fuentes y todas las familias y actividades económicas de manera individualizada.

Naturaleza y alcance del algoritmo

Dada la naturaleza de este trabajo, hemos considerado oportuno expresar los elementos que forman los conjuntos *A* y *B* de manera general, para que el algoritmo posea los atributos necesarios para ser utilizado en el mayor número de ocasiones posible.

Es evidente que cada caso específico comporta el propio nivel de amplitud y composición de los elementos que forman los conjuntos *A* y *B* de incidentes e incididos sobre los que se estudia su gestión de ciberseguridad.

En todo caso, las fases o etapas del procedimiento de cálculo van a mantener su estructura y sus operadores.

Y es en este sentido que, con toda humildad proponemos un algoritmo destinado a la gestión de la ciberseguridad de las energías, cuando se plantea gestionar su captación, distribución, así como la actividad cibernética de las familias y de los distintos actores de la actividad económica.

Como es habitual en nuestros trabajos, vamos a recurrir a técnicas que son propias del pensamiento de la **Escuela de Economía Humanista de Barcelona.**

Así, pues, se hallarán presentes, expresa o tácitamente, el principio de simultaneidad gradual, las nociones de grado o nivel, de playa de entropía, así como los operadores propios de las teorías de la relación, asociación, agrupación y ordenación de la llamada matemática no numérica de la incertidumbre.

Vamos a empezar anunciando las siguientes proposiciones:

-. Existe una gestión de ciberseguridad en la obtención de cada una de las energías limpias A

-. Existe una gestión de ciberseguridad en cada una de las actividades económicas B

-. Existe una gestión de ciberseguridad en la distribución de energía A a las actividades económicas B

Empezamos con la presentación del conjunto *A* de elementos incidentes:

a_1: Ciberseguridad en la obtención de energía solar

a_2: Ciberseguridad en la obtención de energía eólica

a_3: Ciberseguridad en la obtención de energía hidráulica

a_4: Ciberseguridad en la obtención de energía geotérmica

a_5: Ciberseguridad en la obtención de energía maremotérmica

a_6: Ciberseguridad en la obtención de energía de biomasa

a_7: Ciberseguridad en la obtención de energía osmótica

a_8: Ciberseguridad en la obtención de energía con hidrogeno verde

No hay ni que decir, que se podrían añadir otros tipos de energía limpia. En este trabajo nos hemos limitado a aquellas que hemos considerado más asequibles en el entorno del área para la cual este ensayo ha sido elaborado.

Sin pretensión de exhaustividad y únicamente con carácter indicativo, diremos que la gestión de ciberseguridad busca impedir, frenar o resolver ataques tales como los realizados a centrales eléctricas, oleoductos, gaseoductos, plantas de tratamiento de agua, así como a otras fuentes de obtención de energías limpias y sus plantas de producción, como placas fotovoltaicas, embalses, parques de aerogeneradores de energía eólica o plantas para obtener hidrogeno verde.

Las potenciales consecuencias para el futuro de los ciberataques, comprenden una variada gama de situaciones, muchas de ellas de una gravedad extrema, como se ha comprobado tristemente en los sucesos de esta índole ocurridos en los últimos tiempos: acceso ilícito a informaciones sensibles, pérdida de servicios, pérdida de control de los sistemas de trabajo, averías graves en los instrumentos de trabajo, daños humanos y físicos, daños medioambientales e incumplimiento regulatorio, para citar solo las más comentadas en los medios especializados en ciberseguridad.

Pasamos a enumerar, seguidamente, la gestión de ciberseguridad en el conjunto de familias y actividades económicas a las que irán destinadas estas energías, es decir, el conjunto *B* de elementos incididos:

b_1: Ciberseguridad en la industria siderometalúrgica

b_2: Ciberseguridad en la industria de automoción

b_3: Ciberseguridad en promoción y construcción de viviendas

b_4: Ciberseguridad en obras públicas (suministros de agua, energía eléctrica, gas)

b_5: Ciberseguridad en las actividades comerciales

b_6: Ciberseguridad en la agricultura

b_7: Ciberseguridad en la ganadería

b_8: Ciberseguridad en las telecomunicaciones

b_9: Ciberseguridad en la producción de instrumentos digitales

b_{10}: Ciberseguridad en el turismo

b_{11}: Ciberseguridad en el sector financiero

b_{12}: Ciberseguridad en los hogares

Hemos reducido todo cuanto nos ha sido posible los elementos a utilizar del conjunto de incidentes y del conjunto de incididos, limitándolos a ocho y doce, respectivamente. Es suficiente, creemos, para expresar las relaciones de incidencia tomadas de dos en dos mediante una matriz rectangular borrosa $[\underset{\sim}{M}]$ de 8x12 elementos.

En ella se colocan en las casillas correspondientes la valuación que ha realizado un comité de expertos sobre el grado o nivel de incidencia de cada elemento del conjunto de incidentes A sobre cada elemento de conjunto de incididos B, expresado mediante el sistema endecadario en [0,1].

Para tener en cuenta también, como ya hemos expuesto, las incidencias autoinducidas, vamos a construir otras dos matrices, éstas cuadradas pero no necesariamente reflexivas, en la que se colocarán, en la primera, las valuaciones de las incidencias de cada elemento incidente con los demás incidentes, incluyendo la incidencia consigo mismo y en la segunda las valuaciones de las incidencias de cada elemento incidido con los demás incididos, incluyendo la incidencia consigo mismo que, en nuestro caso reflejará el grado o nivel de gestión de ciberseguridad del elemento a_i , x_i, i = 1,2, …, n inmediatamente antes de iniciar la distribución a las actividades económicas destinatarias, b_j , j= 1,2,….,m.

Aún en el caso de una pequeña matriz, como la propuesta de orden 8x12, los flujos potencialmente existentes dan lugar a una gran y tupida red de flujos que la mente humana difícilmente puede retener en su totalidad, sin la ayuda de los instrumentos de Inteligencia Artificial como los por nosotros propuestos[6].

Descripción del algoritmo para la optimización de flujos

Con objeto de evitar un innecesario riesgo de caer en una confusión, vamos a enumerar las etapas del algoritmo que proponemos, junto con las valuaciones o medidas establecidas por la comisión de expertos[7], acompañadas de los operadores que se van a utilizar en cada etapa.

1.- Formación del conjunto A de elementos que actúan como incidentes

$$A= \{a_1, a_2,\ldots a_8\}$$

2.- Formación del conjunto B de elementos que actúan de incididos

$$B = \{b_1, b_2,\ldots, b_{12}\}$$

3.- Construcción de la matriz $[\underset{\sim}{M}]$ de valuaciones (x_i,y_j), i = 1,2,…8; j = 1,2,…12,

Esta fase únicamente comporta la recogida de las informaciones suministradas por el comité de expertos y su colocación en la correspondiente casilla de la matriz.

6 Kaufmann, A. y Gil Aluja, J.: "Models per a la recerca d'efectes oblidats" Ed. Milladoiro, Vigo 1988, pág. 118 (ISBN: 84-404-3657-2)

7 En relación a la figura del experto, se puede consultar una amplia bibliografía. Por nuestra parte recomendamos la obra de Kaufmann, A. y Gil Aluja, J.: "Técnicas especiales para la gestión de expertos", cuyo texto íntegro se halla en la página web de la RACEF. Ed. Milladoiro, Vigo, 1993 (ISBN: 84-404-3657-2)

Una vez realizadas estas tareas se dispone, ya, de la matriz borrosa $[\underset{\sim}{M}]$ de incidencias primarias, y, por tanto, de los grados o niveles de los flujos de gestión de ciberseguridad directos que circulan por la red, desde las fuentes de energía hasta la utilización cibernética de familias de las actividades económicas.

$[\underset{\sim}{M}] =$

$\underset{\sim}{M}$	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}
a_1	0.8	0.9	0.6	0.6	0.7	0.6	0.5	0.4	0.8	0.6	0.8	0.9
a_2	0.6	0.7	0.8	0.5	0.8	0.9	0.6	0.5	0.8	0.7	0.9	0.7
a_3	0.9	0.7	0.6	0.7	0.8	0.5	0.8	0.8	0.6	0.8	0.8	0.6
a_4	0.6	0.6	0.8	0.7	0.6	0.7	0.8	0.6	0.7	0.9	0.7	0.5
a_5	0.5	0.7	0.7	0.6	0.5	0.8	0.6	0.6	0.5	0.7	0.6	0.6
a_6	0.6	0.5	0.7	0.7	0.6	0.8	0.5	0.7	0.6	0.7	0.7	0.8
a_7	0.7	0.8	0.6	0.6	0.7	0.7	0.7	0.6	0.7	0.6	0.6	0.7
a_8	0.8	0.8	0.7	0.9	0.7	0.7	0.8	0.9	0.9	0.6	0.8	0.8

Las incidencias de todos los elementos incidentes a_i / i= 1,2,…8, sobre todos los incididos b_j / j= 1,2,…,12, recogidas en la matriz $[\underset{\sim}{M}]$ se podrían representar mediante una red de incidencias de gestión de la ciberseguridad desde cada incidente a cada incidido, muy simple en comparación con la que tiene lugar, como se verá posteriormente, cuando se incorporan, también, las incidencias autoinducidas.

En este caso de incidencias directas, la mente humana puede, sin más, estimar todos los arcos de la red. En la hipótesis de incorporación en el proceso las incidencias autoinducidas el cerebro "agradece" la ayuda de un algoritmo.

4.- Construcción de la matriz borrosa $[\underset{\sim}{A}]$ de las valuaciones (x_i, x_h) / i, h = 1,2,…,8, de incidencias autoinducidas del conjunto A entre sí.

Las valuaciones de los elementos a_i , i= 1,2, …, n; (x_i , x_i), diagonal principal de la matriz, expresan el grado o nivel de gestión de ciberseguridad que el flujo ha arrastrado **hasta antes** de **iniciar** la transferencia de la gestión de ciberseguridad del conjunto *A* hasta cada una de las gestiones de ciberseguridad de las familias y actividades económicas del conjunto *B*.

En nuestro caso la comisión de expertos les ha asignado los grados o niveles de partida siguientes:

(x_1,x_1)= 0.8, (x_2,x_2)= 0.7; (x_3, x_3)= 0.6; (x_4,x_4)= 0.4; (x_5,x_5)= 0.5; (x_6,x_6)= 0.6; (x_7, x_7)= 0.4; (x_8, x_8)= 0.7

$[\underset{\sim}{A}]$ =

$\underset{\sim}{A}$	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_1	0.8	0.9	0.6	0.5	0.5	0.7	0.6	0.8
a_2	0.6	0.7	0.6	0.8	0.6	0.7	0.6	0.7
a_3	0.8	0.7	0.6	0.6	0.7	0.6	0.6	0.7
a_4	0.4	0.4	0.8	0.4	0.5	0.4	0.3	0.5
a_5	0.3	0.4	0.6	0.7	0.5	0.8	0.7	0.6
a_6	0.2	0.3	0.7	0.7	0.6	0.6	0.7	0.8
a_7	0.4	0.5	0.8	0.6	0.7	0.3	0.4	0.5
a_8	0.5	0.6	0.8	0.4	0.3	0.2	0.5	0.7

5.- Obtención del flujo de incidencias semiacumuladas mediante el operador de convolución max-min.

Las incidencias semiacumuladas se reúnen en una matriz borrosa $[\underset{\sim}{M'}]$, resultado de la convolución máx-min:

$$[\underset{\sim}{A}] \circ [\underset{\sim}{M}]$$

Para ello se halla para cada par (x_i, y_j) i = 1,2,…,8: j =1 ,2,…,12, las valuaciones:

$$(x_i, y_j)' = \bigvee_j \left((x_i, x_h) \wedge \left(x_h, y_j\right)\right)$$

i, h= 1,2,…8

j= 1,2,…,12

En nuestro caso se obtiene:

$[\underset{\sim}{A}] \circ [\underset{\sim}{M}] =$

$\underset{\sim}{A} \circ \underset{\sim}{M}$	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}
a_1	0.8	0.8	0.8	0.8	0.8	0.9	0.8	0.8	0.8	0.7	0.9	0.8
a_2	0.7	0.7	0.8	0.7	0.7	0.7	0.7	0.7	0.7	0.8	0.7	0.7
a_3	0.8	0.8	0.7	0.7	0.7	0.7	0.7	0.7	0.8	0.7	0.8	0.8
a_4	0.8	0.7	0.6	0.7	0.8	0.5	0.8	0.8	0.6	0.8	0.8	0.6
a_5	0.7	0.7	0.7	0.7	0.7	0.8	0.7	0.7	0.7	0.7	0.7	0.8
a_6	0.8	0.8	0.7	0.8	0.7	0.7	0.8	0.8	0.8	0.7	0.8	0.8
a_7	0.8	0.7	0.7	0.7	0.8	0.7	0.8	0.8	0.6	0.8	0.8	0.6
a_8	0.8	0.7	0.7	0.7	0.8	0.7	0.8	0.7	0.7	0.8	0.8	0.7

Una rápida mirada a esta matriz que llamaremos $[\underset{\sim}{M'}]$ nos revela notables diferencias con la matriz de incidencias directas $[\underset{\sim}{M}]$.

Vamos, pues, a aflorar estas diferencias en la matriz siguiente:

$$[\underset{\sim}{O}] = [\underset{\sim}{M'}] \text{ (-) } [\underset{\sim}{M}]$$

Hasta ahora hemos seguido un recorrido destinado a la obtención de un óptimo: **el de la gestión global de la ciberseguridad.** Y para ello se ha adoptado, inicialmente, una escala semántica endecadaria.

En este momento, realizaremos un inciso a efectos **de análisis del resultado obtenido** hasta ahora. Y lo hacemos mediante la diferencia de dos matrices borrosas, lo que va a comportar el tránsito de la escala semántica endecadaria a la eikosienaria.

Al reemprender el camino para obtener el grado o nivel de gestión de ciberseguridad retornaremos a la escala endecadaria.

$[\underset{\sim}{O}]=$

$\underset{\sim}{M}' - \underset{\sim}{M}$	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}
a_1	0	-0.1	0.2	0.2	0.1	0.3	0.3	0.4	0	0.1	0.1	-0.1
a_2	0.1	0	0	0.2	-0.1	-0.2	-0.1	0.2	-0.1	0.1	-0.2	0
a_3	-0.1	0.1	0.1	0	-0.1	0.2	-0.1	-0.1	0.2	-0.1	0	0.2
a_4	0.2	0.1	-0.2	0	0.2	-0.2	0	0.2	-0.1	-0.1	0.1	0.1
a_5	0.2	0	0	0.1	0.2	0	0.1	0.1	0.2	0	0.1	0.2
a_6	0.2	0.3	0	0.1	0.1	-0.1	0.3	0.1	0.2	0	0.1	0
a_7	0.1	-0.1	0.1	0.1	0.1	0	0.1	0.2	-0.1	0.2	0.2	-0.1
a_8	0	-0.1	0	-0.2	0.1	0	0	-0.2	-0.2	0.2	0	-0.1

En líneas generales, se puede decir que las cifras que aparecen en cada casilla como elementos de la matriz $[\underset{\sim}{O}]$ se pueden considerar como el incremento o bien decremento del caudal, es decir, la mejor o peor gestión

de ciberseguridad (caudal que fluye) desde una fuente de energía hasta las actividades cibernéticas de las familias o a una actividad económica como consecuencia de la incidencia autoinducida entre las (en nuestro caso) ocho fuentes de energía , gestionadas cibernéticamente hablando en sí mismas hasta las familias y las actividades económicas, también en sí mismas gestionadas.

Se pueden observar en la matriz $[\underset{\sim}{O}]$ unas relaciones de incidencia en las que el caudal ha aumentado en un flujo igual o superior a 0.3. Se trata, entonces, de rutas de interés de ciberseguridad. Pero más interés existe en aquellas que con valores negativos (inferiores o iguales a -0.1) nos advierten de una pérdida en la gestión de ciberseguridad.

¡Atención! pues, al papel que puede jugar la previsión de una buena gestión y eficaz relación entre los gestores de ciberseguridad de las **fuentes de energía** y entre los que recae la gestión de la ciberseguridad en el proceso de distribución y utilización cibernética .

6.- Elaboración de la matriz borrosa $[\underset{\sim}{B}]$ de incidencias autoinducidas correspondientes a los elementos del conjunto de inducidos b_j / j= 1,2,…,12.

Como es bien conocido, las relaciones entre los gestores de ciberseguridad de las familias y de cada una de las actividades económicas con las demás, también juega un papel importante en las valuaciones de la siguiente matriz $[\underset{\sim}{B}]$, ya que el grado o nivel de **colaboración** puede cambiar de manera sustancial en cada una de estas actividades. En este trabajo, hemos respetado los datos facilitados por nuestra comisión de expertos.

Las informaciones de la comisión de expertos nos ha permitido reunir en la matriz $[\underset{\sim}{B}]$, que reproducimos a continuación, las valuaciones (y_j,y_k) / j, k= 1,2,…,12.

$[\underset{\sim}{B}] =$

$\underset{\sim}{B}$	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}
b_1	0.7	0.8	0.7	0.8	0.6	0.5	0.3	0.8	0.8	0.6	0.7	0.5
b_2	0.8	0.8	0.6	0.7	0.6	0.4	0.8	0.7	0.8	0.7	0.8	0.6
b_3	0.6	0.7	0.6	0.8	0.8	0.3	0.2	0.7	0.6	0.8	0.8	0.8
b_4	0.6	0.7	0.6	0.6	0.4	0.2	0.8	0.7	0.5	0.7	0.7	0.4
b_5	0.5	0.5	0.8	0.7	0.7	0.4	0.3	0.6	0.7	0.8	0.7	0.8
b_6	0.1	0.6	0.2	0.1	0.7	0.4	0.8	0.3	0.3	0.4	0.5	0.3
b_7	0.1	0.2	0.1	0.1	0.4	0.8	0.3	0.3	0.2	0.8	0.1	0.2
b_8	0.8	0.8	0.6	0.7	0.7	0.3	0.2	0.7	0.7	0.8	0.8	0.6
b_9	0.8	0.8	0.7	0.6	0.7	0.2	0.1	0.8	0.8	0.8	0.9	0.7
b_{10}	0.6	0.7	0.6	0.3	0.8	0.6	0.5	0.8	0.6	0.6	0.8	0.7
b_{11}	0.8	0.7	0.7	0.7	0.6	0.5	0.5	0.8	0.8	0.7	0.6	0.8
b_{12}	0.2	0.6	0.7	0.3	0.7	0.1	0.2	0.1	0.4	0.1	0.7	0.4

La existencia de valuaciones bajas, indica, entre otras circunstancias, la poca existencia relacional entre los grupos que forman el conjunto B de incidentes.

Con la construcción de esta matriz $[\underset{\sim}{B}]$ de incidencias autoinducidas por parte de los elementos primariamente inducidos, b_j / j= 1,2,…,12, es decir, de las familias y actividades económicas, se dispone de todas las informaciones numerizadas, imprescindibles para el cálculo del grado o nivel de incidencias totales.

7.- Obtención del flujo de incidencias acumuladas totales

De nuevo, como no podría ser de otra manera, vamos a continuar utilizando el operador de convolución max-min para incorporar los flujos de inci-

dencia autoinducida del conjunto B, $[\underset{\sim}{B}]$, a los que ya se poseían en el flujo de incidencias semiacumuladas $[\underset{\sim}{A}] \circ [\underset{\sim}{M}]$.

Se utiliza, para ello, la siguiente expresión:

$$(x_i, y_j)^* = \bigvee_j \left((x_i, y_j)' \wedge (y_j, y_k) \right)$$

$$i = 1,2,\ldots,8$$

$$j, k = 1,2,\ldots,12$$

Se obtiene:

$[\underset{\sim}{A}] \circ [\underset{\sim}{M}] \circ [\underset{\sim}{B}] =$

$\underset{\sim}{M}^*$	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}
a_1	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8	0.8
a_2	0.7	0.7	0.7	0.8	0.8	0.7	0.7	0.8	0.7	0.8	0.8	0.8
a_3	0.8	0.8	0.7	0.8	0.7	0.7	0.8	0.8	0.8	0.8	0.8	0.8
a_4	0.8	0.8	0.8	0.8	0.8	0.8	0.7	0.8	0.8	0.8	0.8	0.8
a_5	0.7	0.7	0.7	0.7	0.7	0.7	0.8	0.7	0.7	0.7	0.7	0.7
a_6	0.8	0.8	0.7	0.8	0.7	0.8	0.8	0.8	0.8	0.8	0.8	0.8
a_7	0.8	0.8	0.8	0.8	0.8	0.8	0.7	0.8	0.8	0.8	0.8	0.8
a_8	0.8	0.8	0.8	0.8	0.8	0.8	0.7	0.8	0.8	0.8	0.8	0.8

La matriz de incidencias totales $[\underset{\sim}{M^*}]$, no ha sido alterada significativamente en relación con la matriz $[\underset{\sim}{M'}]$, de incidencias semiacumuladas. Aun así, existen unas reducciones que, pueden ser objeto de interés. Los vamos a exponer en la matriz diferencia $[\underset{\sim}{P}] = [\underset{\sim}{M^*}]$ (-) $[\underset{\sim}{M'}]$. De nuevo, retomamos, a efectos de análisis, la correspondencia semántica icosienaria. Veámoslo seguidamente:

$[\underset{\sim}{P}]$ =

$[\underset{\sim}{M^*}]$ - $[\underset{\sim}{M'}]$	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}
a_1	0	0	0	0	0	-0.1	0	0	0	-0.1	-0.1	0
a_2	0	0	-0.1	0.1	0.1	0	0	0.1	0	0	0.1	0.1
a_3	0	0	0	0.1	0	0	0.1	0.1	0	0.1	0	0
a_4	0	0	0.2	0.1	0.1	0.3	-0.1	0	0.2	0	0	0.2
a_5	0	0	0	0	0	-0.1	0.1	0	0	0	0	-0.1
a_6	0	0	0	0	0	0.1	0	0	0	0.1	0	0
a_7	0	0.1	0.1	0.1	0	0.1	-0.1	0	0.2	0	0	0.2
a_8	0	0.1	0.1	0.1	0	0.1	-0.1	0.1	0.1	0	0	0.1

Hemos considerado conveniente realizar esta puntualización, casi banal, para atraer la atención de un aspecto importante del tema que nos ocupa como es la posibilidad de una cierta "complicidad de comportamientos" ante la incidencia entre los elementos del conjunto de incididos *B*, lo que podría conducir a una ligera mejoría en las actividades económicas menos ciberseguras.

Grado o nivel del caudal de incidencias totales

Una simple comparación entre las matrices $[\underset{\sim}{M}]$ de incidencias directas y $[\underset{\sim}{M^*}]$ de incidencias totales nos va ha mostrar que en los diferentes recorridos de los flujos se producen, en no pocos canales, unas diferencias en el grado o nivel del flujo desde un elemento incidente a un elemento incidido. Para "numerizar" esta diferencia basta con utilizar la sustracción entre ambas matrices. En nuestro ensayo hemos hallado como resultado

$[\underset{\sim}{D}]$=

$\underset{\sim}{M}^{*}-\underset{\sim}{M}$	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	b_{10}	b_{11}	b_{12}
a_1	0	-0.1	0.2	0.2	0.1	0.2	0.3	0.4	0	0.2	0	-0.1
a_2	0.1	0	-0.1	0.3	0	-0.2	0.1	0.3	-0.1	0.1	-0.1	0.1
a_3	-0.1	0.1	0.1	0.1	-0.1	0.2	0	0	0.3	0	0	0.2
a_4	0.2	0.2	0	0.1	0.2	0.1	-0.1	0.2	0.1	-0.1	0.1	0.3
a_5	0.2	0	0	0.1	0.2	-0.1	0.2	0.1	0.2	0	0.1	0.1
a_6	0.2	0.3	0	0.1	0.1	0	0.3	0.1	0.2	0.1	0.1	0
a_7	0.1	0	0.2	0.2	0.1	0.1	0	0.2	0.1	0.2	0.2	0.1
a_8	0	0	0.1	-0.1	0.1	0.1	-0.1	-0.1	-0.1	0.2	0	0

La matriz $[\underset{\sim}{D}] = [\underset{\sim}{M}^{*}]$ (-) $[\underset{\sim}{M}]$ hallada, presenta las diferencias entre las llegadas de flujos **directos** cuando transitan por cualquiera de los canales capaces de absorber un mayor flujo superior, sea con los que desembocan a través de los canales directos, sea por los canales indirectos.

Aportación del algoritmo a la gestión de la ciberseguridad

A lo largo de la descripción de las fases del algoritmo hemos comentado, a modo de ilustración, algunos aspectos para los que este procedimiento de cálculo puede ser de eficaz ayuda cuando se trata de adoptar decisiones en el ámbito de la ciberseguridad. Sobre todo en problemas como el por nosotros planteado, de alta complejidad a causa de las múltiples interrelaciones de las incidencias existentes entre los elementos que en él intervienen.

Se habrá podido observar, a diferencia de otros procedimientos de cálculo, que el algoritmo propuesto no pretende alcanzar los objetivos técnicos

habituales, relativos a la naturaleza y ventajas e inconvenientes de las fuentes de energía limpia, sino algo tan consustancial con la ciencia económica, como es la **optimización de la gestión** de la ciberseguridad desde la captación de los recursos energéticos hasta la utilización cibernética por parte de las familias y de las actividades económicas.

El algoritmo elaborado en esta ocasión consta de siete fases –etapas. Para cada una de las cuales se establecen los operadores a utilizar con los datos que, suministrados por la comisión de expertos, incluimos acompañando su descripción.

De esta manera, creemos será sencillo su programación para ser utilizado digitalmente: bastará, entonces, introducir los datos, como ya hemos hecho en otras ocasiones, para obtener en primer lugar los objetivos fundamentales que, en nuestro caso consisten en conocer las incidencias óptimas de la gestión de ciberseguridad entre cada uno de los depósitos de energías limpias; en su tránsito hacia las familias y las actividades económicas y en cada una de ellas. Lo que significa, en definitiva, guiar cada energía a su mejor destino de ciberseguridad.

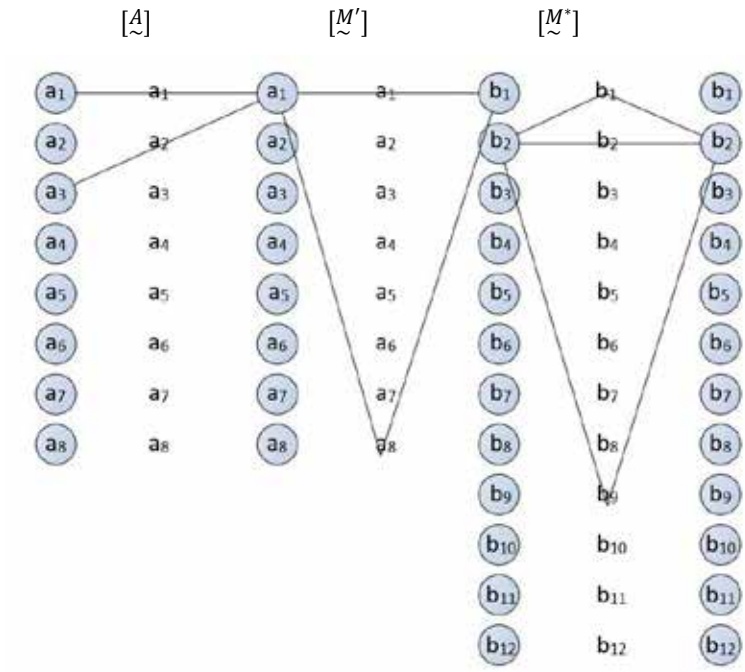
A este respecto puede resultar interesante, como comentamos en el inicio de este trabajo, recurrir a la representación reticular de las relaciones de incidencia en la gestión de ciberseguridad.

Nos limitaremos, en este trabajo, únicamente a un par de incidencias y a representar solo aquellos recorridos capaces de fluir desde una situación iniciar a_i, i= 1,2, …, n, hasta una situación final, b_j, j= 1,2,…, m.

En el primero, la movilidad del flujo de energía provoca una reducción en el nivel final de gestión de ciberseguridad: se trata de la incidencia de la gestión a_1, **ciberseguridad en la obtención de energía solar** sobre la **ciberseguridad en la industria de automoción,** en la que la **incidencia directa** es altísima, 0.9, y, en cambio, con criterio de prudencia (utilización del operador de convolución max-min) los mejores recorridos indirectos **reducen** el nivel de gestión de ciberseguridad en un 0.1 hasta un grado o nivel 0.8.

No procede, en este caso, confiar en la mejora de la gestión de ciberseguridad por el apoyo de b_1, ciberseguridad en la industria siderometalúrgica, de $b_{8,}$ ciberseguridad en las telecomunicaciones o de b_9, ciberseguridad en la producción de instrumentos digitales.

Por el contrario, en el segundo recorrido, el flujo de gestión de ciberseguridad que es baja en la relación directa entre a_1, gestión de la ciberseguridad en la obtención de energía solar y b_8, gestión de la ciberseguridad en las telecomunicaciones, aumenta, sensiblemente, por efecto de su relación con a_8, gestión de ciberseguridad en la obtención de energía con hidrogeno verde, gestión de la ciberseguridad en la industria siderometalúrgica, b_1; ciberseguridad en el turismo, b_{10} o bien, gestión de ciberseguridad en el sector financiero, b_{11}. Lo que resumimos en el grafo siguiente:



$[\underset{\sim}{M}]$	$[\underset{\sim}{M}^*]$	$[\underset{\sim}{M}^*]$ (-)$[\underset{\sim}{M}]$
$(x_1 , y_2)= 0.9$	$(x_1, y_2)^*= 0.8$	$0.8 – 0.9= -0.1$
$(x_1 , y_8)= 0.4$	$(x_1 , y_8)^*= 0.8$	$0.8 – 0.4= 0.4$

Pero es que, además, al programar de tal manera que se dispongan de los resultados parciales, se facilita y se amplía el marco del análisis y consecuencias en la gestión de la ciberseguridad en cada uno de los centros de gestión: fuentes de energía, distribución de energía y utilización cibernética.

No desearíamos finalizar este trabajo sin señalar su dependencia de la tan citada "teoría de los efectos olvidados" de Kaufmann y Gil Aluja. En ella se busca dar solución a lo que se ha dado en llamar "olvidos", para identificar no solo los aspectos de un sistema complejo que la mente humana no suele abarcar por su elevado número y, muchas veces por encontrarse en recónditos lugares de la memoria,. Con los mecanismos establecidos en la reiteradamente citada teoría, se recuperan todas, absolutamente todas, las relaciones de incidencia.

Nos permitimos recordar una característica muy importante que hay que señalar en cuanto a la creación y funcionamiento del algoritmo que proponemos.

En los algoritmos elaborados con la utilización de la "Fuzzy Sets Theory" las magnitudes se mueven dentro del intervalo [0 , 1]. Además, nos hemos acostumbrado, dentro de este intervalo, a la utilización de una **escala semántica endecadaria**.

En este algoritmo, hemos continuado así para hallar la gestión óptima global, desde la obtención de las energías hasta la utilización cibernética final.

Sin embargo, para los procesos de análisis de gestión, hemos incorporado una escala más amplia, que contiene veintiuna relaciones número-concepto que hemos denominado **escala semántica icosienaria** (del griego antiguo, icosi-ena).

Esto nos ha permitido representar las mejoras [0, 1] y los retrocesos [0 , -1] en la gestión de la ciberseguridad desde la obtención y depósito inicial hasta la utilización cibernética final. Solo a los efectos de análisis, la escala semántica icosienaria dará lugar a valuaciones en el intervalo [-1, 1]

También es conveniente señalar unas características de este algoritmo, como acostumbra a serlo de otros algoritmos: su flexibilidad y adaptabilidad a los diferentes escenarios en los que se desea utilizar. Y, esto, tanto en cuanto a la dimensión de los conjuntos de incidentes e incididos, como en el contenido mismo de los elementos de uno y otro.

En un horizonte razonable, incluso a corto y medio plazo, se avisan modificaciones importantes en nuestras sociedades, sin que se puedan avanzar, con mínima precisión, los sentidos que tomarán los acontecimientos que van a cambiar nuestras vidas. Son las horas que nos ha sido dado vivir y en ellas nos debemos acomodar, para gozar de su más jugosos frutos.

Esto es lo que este viejo profesor desearía legar a las futuras generaciones.

Muchas, muchas gracias.

BIBLIOGRAFIA

-. Gil Aluja, J.: "La gestión interactiva de los recursos humanos en la incertidumbre". Ed. Centro de Estudios Ramón Areces. Madrid, 1996. (ISBN: 84-8004-199-4) Existe versión inglesa de Kluwer Academic Publishers 1996 (ISBN: 0-7923-4886-9)

-. Gil Aluja, J.: "Lances y desventuras del paradigma de la teoría de la decisión". Proceedings del III Congreso SIGEF, Buenos Aires, 11-13 de noviembre de 1996.

-. Gil Aluja, J.: "Invertir en la incertidumbre" Ed. Pirámide, Madrid 1997. (ISBN: 84-368-1123-7) Existe versión inglesa de Kluwer Academic Publishers 1999 (ISBN: 0-7923-4886-9)

-. Gil Aluja, J.: "Elements for a Theory of Decision in Uncertainty" Ed. Milladoiro Vigo 1999 (ISBN: 84-605-9437-8) Versión Española del texto en inglés autorizada por Kluwer Academic Publishers. Dordrecht-Boston-London 1999 (ISBN: 0-7923-5987-9)

-. Gil Aluja, J.: "Introducción a la teoría de la incertidumbre en la gestión de empresas". Ed. Milladoiro, Vigo 2002. (ISBN: 84-931-2294-7). Existe versión inglesa con el título: "Fuzzy Sets in the Management of Uncertainty". Ed. Springer-Verlag. Berlín, Heidelberg, Nueva York (ISBN: 3-540-20341-9)

-. Gil Aluja, J.: "Las revoluciones tecnológicas frente al mandato biológico" en la obra colectiva "Desafíos de la nueva sociedad sobrecompleja: humanismo, transhumanismo, dataismo y otros ismos", Ed, RACEF. Barcelona 2019, (ISBN: 978-84-09-08674-0)

-. Gil Aluja, J.: "En el horizonte del poshumanismo" en la obra colectiva "Desafíos de la nueva sociedad sobrecompleja: humanismo, transhumanismo, dataismo y otros ismos", Ed, RACEF. Barcelona 2019, (ISBN: 978-84-09-08674-0)

-. Gil Aluja, J.: "Papel de la memoria en la armonía entre territorios: el Algoritmo de Portugal" en la obra "Complejidad Económica: una Península Ibérica más unida para una Europa más fuerte" Ed. RACEF, Barcelona 2019, (ISBN: 978-84-09-12599-9)

-. Gil Aluja, J.: "Un ensayo para solución al problema migratorio a través de la Inteligencia Artificial" en la obra "Migraciones". Ed. RACEF Barcelona 2020, (ISBN: 978-84-09-18254-1)

-. Gil Aluja, J.: "Vejez y revolución digital" en la obra: "La vejez: conocimiento, vivencia y experiencia". Ed. RACEF, Barcelona 2021, (ISBN: 978-84-09-37745-2)

-. Gil Aluja, J.: "Economic Humanism Self-indiced in the Circular Economy", en la obra colectiva de Rodríguez García, M. de P. y otros. Ed. SIGEF, 2021 .LNNS 384, 2022

-. Gil Aluja, J.: "Un caudal óptimo de recursos para la descarbonización" en la obra: "¿Por qué no un mundo sostenible? La ciencia económica va a su encuentro". Varios autores. Ed. SIGEF, Barcelona, 2023 (ISBN: 978-84-09-48026-5).

-. Gil Aluja, J. y Gil Lafuente, A.M.: "Algoritmos para el tratamiento de fenómenos económicos complejos". Ed. Universitaria Ramón Areces, Madrid, 2007 (ISBN: 84-8004-787-6) La Versión inglesa tiene el ISBN: 978-3-942-24812-2.

-. Gil Lafuente, J.: "Marketing para el nuevo milenio. Nuevas técnicas para la gestión comercial en la incertidumbre". Ed. Pirámide, Madrid, 1997. (ISBN: 84-368-1088-0)

-. Gil Lafuente, J.: "Algoritmos para la excelencia. Claves para el éxito en la gestión deportiva". Ed. Milladoiro, Vigo 2002 (ISBN: 84-93-1229-3-9)

-. Gil Lafuente, J.; Mulles A.; Solé Moro, M. L.: "Un algoritmo en base a expertones para facilitar la selección de restaurantes según la tipología de clientes de un hotel" Actas del XXXIII AEDEM anual Meeting. Sevilla, 2019. Pág. 1816-1843.

-. Kaufmann, A.: “Introduction à la théorie des sous-ensembles flous”. Ed. Masson. París 1973 (ISBN: 2-225-45804-9) Existe una versión española de Ed. CECSA, México 1982 (ISBN: 968-26-0289-1)

-. Kaufmann, A. y Gil Aluja, J.: “Introducción de la teoría de los subconjuntos borrosos a la gestión de las empresas”. Ed. Milladoiro, Santiago de Compostela, 1986 (ISBN: 84-398-7630-0)

-. Kaufmann, A. y Gil Aluja, J.: “Modelos para la investigación de efectos olvidados” Ed. Milladoiro, Vigo, 1988 (ISBN: 84-404-3657-2)

-. Kaufmann, A. y Gil Aluja, J.: “Técnicas especiales para la gstión de expertos”. Ed. Milladoiro, Vigo 1993 (ISBN: 84-404-3657-2)

-. Kaufmann, A. y Gil Aluja, J.: “Models per a la recerca d’efectes oblidats”. Ed. Milladoiro, Vigo, 1988. (ISBN: 84-404-3657-2)

-. Kaufmann, A. y Gil Aluja, J.: “Grafos neuronales para la economía y gestión de empresas”. Ed. Pirámide, Madrid 1995. (ISBN: 84-318-0917-3)

-. Prigogine, Ilya: “La fin des certitudes”. Versión española con el título “El fin de las certidumbres”. Ed. Taurus, Buenos Aires 1997. (ISBN:84-306-0025-6)

-. Zadeh, L. A.: “Fuzzzy Sets”. Information and Control. 8 de junio de 1965.

CYBERSECURITY CONTEXT IN SERBIA: LEGISLATIVE AND STRATEGIC FRAMEWORK

Dr. Dobrica Milovanović
Miembro de la Barcelona Economics Network de la Real Academia de Ciencias Económicas y Financieras

Abstract:
Cyber security is a real issue and a potentially great threat for every country. Along with the development of technology, one of the characteristics of modern society is the occurrence of criminal acts precisely through the use of the same technology to commit criminal acts. The frequency of cyber attacks is increasing globally. Serbia has a substantial commitment to addressing the challenges of cybersecurity and providing critical cyber infrastructure. In recent years, Serbia has introduced a number of strategic frameworks and organizational structures in the field of cybersecurity. A report assessing the country's cybersecurity conducted by the World Bank says that Serbia performs well across many areas of cybersecurity capacity and outlines the country's relatively strong legal framework in relation to cybersecurity. However, it seems that there are many weaknesses in the implementation which lags behind the threats that are evolving in cyberspace. Along with the development of technology, new forms of challenges, risks, and threats are emerging that are not covered by the current criminal legislation. Therefore, there is a crucial need for the state authorities to be prepared to respond to any challenge, risk, or threat quickly and effectively while, at the same time, respecting human rights and the rule of law. It is necessary to work actively to raise awareness of the fact that cybersecurity is a human rights issue. There is a need to promote an open, free, and stable cyberspace realm where the rule of law applies fully and human rights and fundamental freedoms are respected. In order to achieve these goals it is necessary

to build an environment of trust, in particular between the state and the private sector.

Keywords: cybercrime, *cybersecurity, legislation, privacy, protection*

1. INTRODUCTION

Cybercrime is the commission of crimes in which the computer is the mean or object of the criminal act and in which all potential victims are independent of age, gender and place of residence. The most common types of cybercrime are online fraud, cyberbullying, cyber deviance, cyber paedophilia, cyber pornography, the crypto market, etc. Cybersecurity is an area of vital interest for any country. It encompasses the detection and prevention of cyber attacks, responses to such attacks, and the protection of data and information of all kinds against the risk of being stolen or compromised, which poses threats to national security and to the security of organizations, communities, and individuals. This includes personal and health-related information, sensitive data of all kinds, intellectual property, and information held in government, business, and industry computer systems. An appropriate cybersecurity strategy is one of the most essential tools for keeping a country, its businesses, and ultimately its people safe.

The question is how many users are aware of the dangers of using the internet and the possibility of becoming a victim of a cybercrime. The existence of a culture of security today represents the basic principle of human security, along with the rule of law. Privacy is a human right and guarantor of human dignity, and is key to maintaining personal security, protecting identity, and promoting freedom of expression in today's digital environment.

Cyber attacks are now a part of daily life in Serbia. As the number of internet users increases, so does the number of potential victims of cybercrime and the obligation of states to protect citizens. Official statistics indicate an increasing trend in the number of cyber attacks and cybercrime cases. In 2020 there was about 26 million cyber attacks on information and communication

technology (ICT). The citizens also experienced considerable violations of their right to privacy and personal data during the pandemic. For sure, threats posed by the internet and social networks are likely to intensify and become more complicated in the future.

The data on the targets of the attacks show that the most frequent targets are legal entities at 23%, then state institutions at 21%, individuals at 12% and the rest are various organisations, educational institutions, and the financial sector.

Only since the beginning of 2022, there have been several hackers' attempts to steal the identities and data of users of some banks, the national cadastre and the Post of Serbia. Very often hackers shared information about bombs planted in many institutions, which not only caused a very big public concern, but also temporarily disabled their regular function.

The anonymity that cybercrime affords to perpetrators makes it even more difficult to identify the perpetrator. In some situations, an additional problem in identifying the computer used is identifying the person who used the computer to commit the crime. Some real-world crimes take place in the virtual world, so predators are increasingly hiding behind computers and anonymity rather than lurking in predator playgrounds. The difficulty in establishing the identity of the perpetrator is one of the reasons for a large number of cybercrimes, precisely because modern technology allows for a high level of anonymity. In addition, one of the ways of detection is to analyse similar cyberattacks to establish a correlation between them.

Official information from the Government of Serbia, confirmed by the Report conducted by the World Bank, says that Serbia performs well across many areas of cybersecurity capacity. The assessment found that Serbia has a substantial commitment to addressing the challenges of cybersecurity and highlights its cybersecurity policy, which enables the country to create mechanisms that can ensure the protection of critical infrastructure.

2. CYBERSECURITY IN SERBIA

2.1 Legislative and strategic framework

In 2005, the Law on the Organisation and Competence of State Bodies in Combating High-Tech Crime was adopted in the Republic of Serbia (Narodna skupština, 2009). According to this Law on Procedures in Crimes where Computers and Computer Systems are the Object or Means of Execution, the Prosecutor General's Office in Belgrade is responsible for the procedure, i.e., the Special Department for Combating High-Tech Crime. The department becomes active in the preliminary proceedings at the request of the specialist agency for combating high-tech crime. The main problem with this service is the lack of human resources. The trial in these cases is within the jurisdiction of the Supreme Court in Belgrade, where a special department to combat high-tech crime should be established and where priority should be given to judges with special knowledge of information technology.

In 2016 the Government of Serbia started to work together with the private sector and civil society more seriously to define the legislative and strategic framework for the area of ICT security. This was regulated by the umbrella Law on Information Security defining the rights, duties, and responsibilities of all legal entities and state authorities managing and using ICT systems.

In 2019 this framework was revised taking into consideration practical experience and European Union directives and guidelines. Having in mind the importance of this law, the by-laws were introduced in the area of cybersecurity, such as the laws regulating personal data protection, critical infrastructure, electronic communication, and other relevant areas. Cybersecurity also includes the area of cybercrime, regulated by a separate legal and strategic framework. Experts describe the quality of the legal framework as solid, even emphasizing that Serbia is the most advanced in the region.

However, implementation lags behind the threats that are evolving in cyberspace. With the development of new technology, new forms of challenges,

risks, and threats are emerging that are not covered by the current criminal legislation.

The opponents, such as some experts and civil society organizations dealing with human rights, think that there is a need to modify how the *Criminal Code* defines criminal offences in the area of high-tech crime, especially offences that do not directly stem from high-tech crime and that cannot be prosecuted *ex officio* but remain within the private lawsuit.

They emphasize that the law established inequity regarding age, since juvenile persons enjoy a higher degree of protection. In case their rights are violated, national authorities are more likely to intervene *ex officio*, while ad*u*lts must initiate a private lawsuit. They also suggest introducing new criminal offences, such as sharing intimate images of women without their consent.

Experts and organizations dealing with human rights propose a special legal definition of criminal offences to be prosecuted ex officio. They suggest the need to introduce new criminal offences, such as the non-consensual sharing of intimate images targeting women.

With regard to the strategic framework for ICT security, a new strategy was endorsed, titled the Information Society and Information Security Development Strategy of the Republic of Serbia for the period 2021-2026, which is aligned to the EU Network and Information Security Directive. In the meantime, the Serbian government has endorsed the Strategy for the Development of Artificial Intelligence for the period 2020-2025, which reflects the state's tendency to incorporate advanced technologies into its work.

Although from the perspective of the *Ministry of Information and Telecommunications*, information security, digitalization, and e-commerce are processes that are linked, the opponents highlight the problem that the processes of digitization and development of ICT security, which take place in parallel, are not integrated enough, but greater focus was placed on developing a digital society, rather than ICT security.

Also, the objections are that Cybersecurity is often understood in terms of national security and is embedded in policies related to national security and military doctrines. The main architects of the ICT security system did not, however, apply a national security approach when defining the policies and laws seven years ago, which impacted the system's structure. Nevertheless, the second National Security Strategy of the Republic of Serbia (94/2019-13) recognizes that the development of modern technologies and their omnipresence in society increases the risk of high-tech crime and threats to ICT systems. In the present security environment, particularly since the outbreak of war in Ukraine, cyber warfare and the protection of critical infrastructure is viewed as an integral part of national security at the international and European level. In the future, this could lead to changes in strategic thinking and/or institutional arrangements.

2.1 The actors in cybersecurity area

The state administration bodies recognized under the national cybersecurity strategy are the *Ministry of Information and Telecommunications*, *Regulatory Agency for Electronic Communication and Postal Services* (RATEL) and its *Computer Emergency Response Team* (CERT), as well as *the Serbian government's Coordination Body for Information Security Affairs*.

The Ministry proposes laws and strategies in this area and is the main institution responsible for implementing activities related to ICT security in Serbia.

RATEL is an independent state agency within which the National Centre for the Prevention of Security Risks in ICT Systems of the Republic of Serbia (nCERT) also operates. According to the Law on Information Security the nCERT is responsible for collecting and exchanging information about risks for ICT systems, as well informing, supporting, warning, and advising those in charge of ICT systems, as well as the wider public. Besides the nCERT, other authorities have their respective CERTs, such as the MoI, the Security Intelligence Agency (BIA), and the Serbian Army.

In accordance with international instruments and the obligation of the Republic of Serbia to achieve international cooperation and data exchange in the field of high- tech crime, the bodies responsible for international cooperation and establishing contacts have been designated, namely the *Special Prosecutor for High-Tech Crime*. Therefore, the key actors in the area of high-tech crime are the *Ministry of Interior* (MoI) and the *Special Prosecutor's High-Tech Crime* and the *Department for Suppression of High-Tech Crime*. However, the number of staff is insufficient, given that the Special Prosecutor's Office had 4,769 registered cases in 2020 – a 25 per cent increase compared with 2019.

2.2 The cybersecurity network

Significant supporters in the area of cybersecurity include the international community – primarily the Organization for Security and Co-operation in Europe (OSCE) Mission to Serbia and the Geneva Centre for Security Sector Governance (DCAF) – and civil society, which was responsible for encouraging cooperation between state authorities, citizen associations, the academic community, and business operators.

The Cybersecurity Network, which is recognized by the *ICT Security Development Strategy* facilitates the exchange of information, knowledge, and practices; acts as a support group in case of cybersecurity incidents; and serves as a potential partner for cybersecurity programmes and projects. The network is recognized by the Information Society and ICT Security Development Strategy, and its representatives manage the working group of the Coordination Body for ICT Security Affairs, which has institutionalized its links with the state.

The task of the working group is to provide support to the state in implementing the strategy and to monitor cybersecurity projects at the national and regional level. In the upcoming period, the network will focus on training and empowering young talents in Serbia in the area of cybersecurity, through the Cyber Hero programme. This programme is implemented with the support

of relevant state institutions, higher education institutions, associations, and businesses.

2.3 Challenges and shortcomings

RATEL, more precisely nCERT, has published a comprehensive yearly report on significant ICT system incidents that occurred in 2020. The report states that around 26 million incidents were recorded, the most common being attempts to hack the ICT system (17,332,830) and unauthorized data collection (8,470,838).

The lack of personnel with specific cybersecurity knowledge and experience in cybersecurity, especially IT experts and chief information officers, hinders government efforts to protect ICT systems more effectively.

Since digitalization is at the top of the political agenda, the government strategically allocates more funds for developing digital services development and investing in people who build and maintain these services. The Office for IT and eGovernment has thus recruited 200 people for the development of digital services using funds from the World Bank, but no cybersecurity experts. Besides this, the situation is compounded by the difficulty of attracting and retaining IT experts within state institutions because the IT labour market offers better remuneration and career development opportunities.

One particular challenge is that many high-tech crime cases exceed the statute of limitation even before they reach court due to the untimely response of the injured parties, as well as the authorities during the evidence-collection phase. The cybercrime penal policy is also lenient, and the criminal offence of having accessed a protected computer without unauthorized, for example, is liable to lead to a prison sentence of up to one year.

Public discussions have mostly focused on state or corporate cybersecurity instead of human security, while parliamentarians often used pub-

lic hearings to praise the government rather than scrutinize it. It is worth stressing that almost all public discussions on cybersecurity have been supported by foreign embassies and international development organizations, highlighting the lack of interest among lawmakers to address a topic that is in the public interest.

3. CYBERSECURITY AND HUMAN RIGHTS FRAMEWORKS

Although some research indicates various forms of threats to the rights and freedoms of marginalized groups in Serbia involving the use of modern technologies, the strategic and legal framework in the area of ICT security does not recognize the impact of these technologies on various social groups, other than children and youth.

Additional standards for human rights protection were included in the national legislation to align with not only the EU directives but also those of the Council of Europe protocols. In May 2022, Serbia was among the first countries to sign the Second Additional Protocol to the Council of Europe Cybercrime Convention on enhanced cooperation and the disclosure of electronic evidence. The protocol is significant because it strengthens states' cooperation with the private sector to protect the rights of all internet users and to collect electronic evidence more efficiently, in accordance with technological developments and new forms of cybercrime.

One of the main challenges in the human rights sphere is the fact that the Serbian authorities are using European integration as a pretext for frequent amendments to the legal framework; as a result, the generation of new regulations often means a step backwards for the civic rights and liberties that have already been achieved. There are also emerging global challenges, such as the war on terrorism and the ongoing war in Ukraine, which could facilitate the expansion of the power and authority of state security actors in cyberspace at the expense of human rights.

3.1 Cybersecurity, the right to privacy and its violation

The first Law on Personal Data Protection was adopted in 2008 but replaced by an entirely new law in 2018. Cybersecurity and legal experts flag the short time frame given for harmonization (9 months) of various state authorities and entities with the GDPR, which makes its implementation difficult, thus further jeopardizing adequate personal data protection.

The key independent state authority responsible for the protection of privacy and personal data is the Commissioner for Information of Public Importance and Personal Data Protection. The commissioner is responsible for initiating oversight procedures regarding the work of state institutions and private companies involved with data processing, whether as data handlers or processors. The national authorities are obliged to notify the commissioner if an incident occurs. Following the adoption of the Law on Personal Data Protection, the commissioner is entitled to initiate misdemeanours proceedings against the state authority and other private entities processing personal data, and the Misdemeanour Court is competent to rule on these cases. According to the GDPR, the fines for violating the right to privacy in the EU can be up to 20 million euros, or 4 per cent of the company's annual turnover, which has not been the case in Serbia so far. The fines envisaged for the violation of legal provisions are from EUR 50 to EUR 8,500.

It can be said that Serbia is a country with a long history of compromising personal data. In the past seven years, there have been serious cases involving violations of the right to privacy, the leakage of data from state and private institutions, as well as the misuse of personal data. Besides citizens' poor knowledge in how to protect their personal data and digital rights, violations of the right to privacy most often occur due to neglect and serious omissions in the work of state authorities and private companies.

The first wave of the COVID-19 pandemic in Serbia in 2020 coincided with the first case of an attack on critical infrastructure, with several incidents

occurring in a row, causing massive leakage of data on the health status of patients in Serbia's public and private health systems.

At the beginning of 2021, the medical records of Medigroup patients were leaked to the media and revealed that many former and incumbent officials, as well as celebrities, were being treated within a private health care system. In June 2022, a telecommunication company Telekom Srbija responsible for an electronic school diary system was found to have failed to adopt rules and procedures related to data security in accordance with the law. As a result, this company have personal data on all students in Serbia, including their health records. Despite a data confidentiality clause in their contracts, the Ministry of Education, Science and Technological Development has not adopted rules and procedures related to information security, i.e. security act, in accordance with the Law on Information of Security.

In several other cases, the state intelligence service (BIA) was found to be responsible for leaking documents from government electronic records through the pro-government media.

In recent years, Serbia has seen an increase in digital surveillance performed by state actors. According to media and investigative reports, state security institutions have procured many digital surveillance tools, including the most intrusive equipment capable of secretly penetrating and controlling users' devices and analysing huge amounts of data in detail.

3.2 Cybersecurity and anti-discrimination

Over the last three years, the crime of 'endangering security on the internet' has increased in the country. According to the SHARE Foundation monitoring report, the most common violations of digital rights and freedoms in Serbia are pressure (due to expression of opinions and activities on the internet), insults and unfounded accusations, as well as manipulation and propaganda within the digital environment.

Citizens and journalists are the most frequently targeted parties, whereas the most common assailants are individuals or unknown persons. The number of attacks against journalists and dissenters, and violations of digital rights and freedoms increased between 2014 and 2019, and reached extreme levels during the pandemic. The fact that these attacks have almost become normalized is worrying, and the absence of sanctions for this type of crime only leads to their increase.

Chart 1. The five most common types of cybercrime in Serbia

Source: Republic Public Prosecutor's Office

Attacks on journalists and the media are fairly well documented and presented in reports by independent state bodies and national and international NGOs. There have also been numerous cases in which employees in state and private companies, trade union activists, as well as legal experts in the judiciary, have been fired or mobbed at work due to their posts on social networks.

The legislative framework for gender equality and anti-discrimination was first developed and approved in 2009. The second set of strategic documents and legal regulations, however, took into account the development of modern technologies and their influence on women and girls. The new Gender Equality Law, adopted in 2021, specifies that gender equality in the area of ICT and information society must:

- Promote ICT and the advantages of using modern technologies among women and girls;

- Ensure a gender balance and equal opportunities for engaging with ICT, as well as mainstream gender in processes related to the financing of these activities.

The law prescribes specific measures for the authorities to take to mitigate the digital gap between women and men, to ensure a balanced representation of women in ICT, and to improve the socio-economic position of women by allowing them to requalify or receive additional training in ICT, as well as by educating girls and young women in science, technology, engineering, and mathematics (STEM).

The legal framework and the newly approved Gender Equality Strategy for the period 2021-2030 recognize the benefits of applying technology for innovation and development purposes.

4. CONCLUSION AND RECOMMENDATIONS

With regard to the fight against cybercrime, normative regulations have been adopted in the Republic of Serbia, which satisfactorily regulate this area and are harmonized with the international instruments of the European Union. Despite a solid legal framework, Serbia's fight against cyber attacks and crime progresses slowly due to the chronic lack of qualified staff, as well as the politicized priorities of the competent institutions. The criminal justice system is not keeping pace with advances in technology; consequently, new forms of cybercrime, where computers or computer networks are used as a means or method of execution, remain outside the criminal law framework. Insufficient training and/or knowledge about cybersecurity among all actors – primarily judges, lawyers, and police officers – leads to a large number of unprocessed 'high-tech' crimes.

Certain individuals and groups, such as women, LGBT people, journalists, and human rights defenders, are particularly vulnerable to threats posed by cybercrime, yet they are not mentioned in strategic documents related to cybersecurity. This is due to the limiting state- or corporate-centric understanding of cybersecurity, as well as the insufficiently inclusive process of developing political documents and legal regulations. As a result, most strategic documents appear to be gender neutral, but the number and type of violations of digital rights and freedom in Serbia is in fact alarming. While state bodies are somewhat effective in protecting critical infrastructure against cyber attacks, the general willingness to tolerate massive violations of citizens' digital rights is worrying.

Recommendations

- The state authorities and the competent institutions should strengthen the infrastructure as well as individual and organizational cybersecurity capacities in order to perform their tasks effectively.
- There is a need to move from a state- or corporate-centric approach to cybersecurity to one that is more human-centric, given the impact it has on not only individuals but also national security and the corporate economy.
- *The Criminal Code* should be amended to clearly define the sharing of intimate images and videos without their consent as a criminal offence. Criminal offences involving the unauthorized collection of personal data, on a large scale, should be prosecuted ex officio.
- Organizations representing marginalized groups in Serbia must be involved in the development of new cybersecurity strategies and laws to ensure that documents reflect their needs.
- A new action plan should be developed for the implementation of the Strategy for Combating High-Tech Crime.
- The use of digital technology for the enforcement of sentences also requires the constant training of employees because the constant advances in tech-

nology also go hand in hand with the use of the same in the area of enforcement of sentences.

- Judges and attorneys dealing with cybercrime cases should have continuous training to avoid problems in proceedings owing to insufficient knowledge of the subject matter.
- The infrastructure capacities, the number of employees, and the technical equipment of the Special Prosecutor's Office for High-Tech Crime should be increased to allow it to perform its tasks effectively.
- Parliamentary oversight in the cybersecurity area should be strengthened and expert support provided to representatives in the new convocation of the assembly – especially to future members of the Committee for Education, Science, Technological Development and Information Society; the Defence and Internal Affairs Committee; as well as the Security Services Oversight Committee.
- Cooperation between governmental, private and public sectors and civil society, must be strengthened bearing in mind that with the development of new technologies, security challenges, risks and threats are constantly increasing.
- The general public should be broadly educated about the various forms of cybersecurity crime and how to protect themselves from these crimes
- The competent ministries, as well as the donor community, should invest funds in programmes of civil society organizations that represent marginalized groups and aim to increase digital literacy and strengthen individual and organizational cybersecurity capacities, especially in the fight against online violence.
- There is a need to strengthen the civil society response and build a wider coalition between women's organizations, the LGBT+ community, Roma associations, and so forth, and for cyber experts to pressure the government to end impunity regarding online violence.

REFERENCES

Abu, A., & Israt, J. (2020). Causes of cybercrime victimization: A systematic literature review. International Journal of Research and Review, 7(5), 89–98. https://www.ijrrjournal.com/IJRR_Vol.7_Issue.5_May2020/IJRR0015.pdf

Bjelajac, Ž., & Filipović, A. (2021). Specific characteristics of digital violence and digital crime. Pravo – teorija i praksa, 38(4), 16–32. https://doi.org/10.5937/ptp2104016B

Bjeloš, M., Čečen, B., Elek, B., Grujičić, G., Hercigonja, S., Ignjatijević, M., Ignjatović, T., Igrutinović, M., Jovanović, M., Krunić, J., Macanović, V., Nenadić, N., Pavlović, M., Pejić Nikić, J., Petrović, P., & Teofilović, I. (2021). PrEUgovor alarm report on the progress of Serbia in Chapters 23 and 24. Belgrade Centre for Security Policy & Transparency Serbia.

Choi, J, Lee, S., & Dittmann, L. (2022). The Relationship between parenting practices and cyberbullying perpetration: The mediating role of moral beliefs. International Journal of Cybersecurity Intelligence & Cybercrime, 5(1), 4–22. https://vc.bridgew.edu /ijcic/vol5/iss1/2

Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA. The European Parliament & the Council of the EU. Official Journal of the European Union, L 335. https://eur-lex.europa.eu/legal- content/EN/TXT/?uri=celex%3A32011L0093

Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. The European Parliament & the Council of the European Union. Official Journal of the European Union, L 218/8. https://eur-lex.europa.eu/legal- content/EN/TXT/?uri=celex:32013L0040

Government of Republic of Serbia (2018). Strategy for the fight against high-tech crime for the period 2019-2023. Službeni glasnik RS, broj 71. http://www.pravnoinformacionisistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2018/71/1/reg

Mali, P., Sodhi, J.S., Singh, T., & Bansal, S. (2018). Analysing the awareness of cyber crime and designing a relevant framework with respect to cyber warfare: an empirical study, International Journal of Mechanical Engineering and Technology, 9(2), 110–124. http://iaeme.com/Home/issue/IJMET?Volume=9&Issue=2

Me, G., & Pesticcio, L. (2022). Tor black markets: economics, characterization and investigation technique. In H. Jahankhani (Ed.), Cyber criminology, advanced sciences and technologies for security applications (119–140). Springer Nature Switzerland.

Ministry of Interior of Republic of Serbia. (2021). Informator o radu [Informer on work]. http://mup.gov.rs/wps/wcm/connect/0021cb85-5d11-4cb1-ad7e-e0a124a7ab41/IOR%2Bmart%2Bcirilica2021..pdf?MOD=AJPERES&CVID=nycATmk

N1 Beograd. (2022). Continuation of the Armageddon action: 14 people were arrested for child pornography. https://rs.n1info.com/vesti/nastavak-akcije-armagedon-uhapseno-14-osoba-zbog-decje-pornografije/

Narodna skupština Republike Srbije [Narodna skupština]. (2019). Krivični zakonik [Criminal Law]. (Službeni glasnik Republike Srbije, broj 85/2005, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019). https://www.paragraf.rs/propisi/krivicni-zakonik-2019.html

Narodna skupština Republike Srbije (2009a). Law on the organization and competence of state bodies for the fight against high-tech crime, Službeni glasnik Republike Srbije, broj 61/2005 i 104/2009). https://www.paragraf.rs/propisi/zakon_o_organizaciji_i_nadleznosti_drzavnih_organa_za_borbu_protiv_visokotehnoloskog_kriminala.html

Narodna skupština Republike Srbije. (2009b). Law on the ratification of the Convention on high-tech crime. Službeni glasnik Republike Srbije, broj 19/2009. http://www.podaci.net/_z1/2129877/Z-pkvkri03v0919.html

Petrović, A. (2021). Interview: Branko Stamenković, special prosecutor for high-tech crime "Kika's law" cannot be considered in the "cyber" world.

Politika. https://www.politika.rs/sr/clanak/495574/Kikin-zakon-ne-moze-da-se-razmatra-u-sajber-svetu

Pournouri, S., Zargari, Sh., & Akhgar, B. (2022). Predicting the cyber attackers; A comparison of different classification techniques. In Ha. Jahankhani (Ed.), Cyber criminology, advanced sciences and technologies for security applications (pp. 169–181). Springer Nature Switzerland.

Sabillon, R., Cano, J, Cavaller, V., & Serra, J. (2016). Cybercrime and cybercriminals: A comprehensive study. International Journal of Computer Networks and Communications Security, 4(6), 165–176.

Sallavaci, O. (2022). Crime and social media: Legal responses to offensive online communications and abuse. In H. Jahankhani (Ed.), Cyber criminology, advanced sciences and technologies for security applications (pp. 3–23). Springer Nature Switzerland.

Stamenković, B., Živanović, S., Paunović, B., & Stevanović, I. (2017). Vodič za sudije i tužioce na temu visokotehnološkog kriminala i zaštite maloletnih lica u Republicu Srbiji [Guide for judges and prosecutors on the topic of high-tech crime and the protection of minors in the Republic of Serbia]. Save the Children in North West Balkans, Sarajevo.

Stošić, L.V. & Janković, A.V. (2022). Cybercrime in the Republic of Serbia: Prevalence, situation and perspectives. Kultura polisa, 19(4), 82–99.

DEEP LEARNING AND EXPLAINABLE AI APPROACHES TO AUTOMATIC VULNERABILITY DETECTION AND CLASSIFICATION FOR IMPROVED CYBER-RESILIENCE

Antonia Russo
University Mediterranea of Reggio Calabria

Francesco Carlo Morabito
Miembro de la Barcelona Economics Network de la Real Academia de Ciencia Económicas y Financieras

Abstract
Cyber-resilience is becoming a critical parameter that measures how an organization can adapt to a continuously changing and challenging cyber-world. This concept also reflects how an organization is willing to improve and offer services ever and ever able to protect its clients' security, privacy, and safety. In a digital society, the management of vulnerabilities is thus fundamental for any organization. However, on the other side, a cyber-resilient society is based on data-driven decisions which often are represented in black-box models. In this paper, Deep learning and explainable AI approaches are investigated as a possible integration of the vulnerability management process, with special reference to the simplification in discovering vulnerabilities, classifying them, and proactively improve the organization's resilience.

Introduction

We live in the society of Information and Communications Technologies (ICT) where digital transition is proposing as the backbone of Europe's economy. The present digital society guarantees lot of novel opportunities for citizens, but also at the governments level to provide access to public services, and for enterprises and businesses by promoting economic growth. These

evident opportunities associated to connecting and participating in the Internet economy are enticing countries and corporations to further expand their digital footprint. They are embedding ICTs into their networked environments and infrastructures, and accelerating access to Internet, broadband networks, mobile applications, IT services, software, and hardware.

Yet, the above mentioned economic opportunity of the extensive use of networks is at risk. The same open nature of the Internet that facilitate the dissemination of data and relevant information, has also exposed our society to cybercrime, hacktivism, service disruption, and destruction of critical digital property. Malicious cyber activities degrade economic progress and threaten national security by undermining the availability, integrity, and resilience of the Internet infrastructure.

Facing the raise of adversarial cyberattacks is both an economic and national security imperative. The Internet infrastructure, services, and delivery to citizens are vulnerable to malicious manipulations. Their economic modernization, and the related security depend on being able to protect the Internet and its access. How can we deal with the trade-off between the need for security and the need for economic growth? Investing in the resilience of the core infrastructure and systems it is now a priority.

On the other side, artificial intelligence and machine learning can effectively contribute to achieving cyber resilience. Indeed, security solutions generate massive data that can be analyzed to individuate or foresee behaviors and risks to improve organizations' ability to adapt and respond to vulnerabilities and attacks.

The relevance of a cyber-resilient society

The modern critical infrastructure systems impact on our lives, from transportation, cities, health, tourism and leisure services. Information and communication technologies pervade all of the systems. That's why cyber-resilience

can modify our perception and ability regarding the response to adversarial cyber-attacks. The same can be said, at the societal different scale of communities, cities, and countries. Resilience is reported as the UNESCO's Sustainable Development Goal 11 "Sustainable cities and communities", which is interpreted as a sort of umbrella for our future societies.

The challenges we face as individuals and communities worldwide in unstable and adverse contexts are pushing us to become ever and ever resilient people able to adapt to changes and learn from crises. Similarly, cyber-resilence aims to help organizations survive and adapt to adverse conditions by developing the ability to evolve the security posture and anticipating new attack vectors.

A cyber resilient enterprise can be defined as one capable to detect, prevent, limit and recover from a potential high number of serious threats against data, applications and IT infrastructure.

Cyber resilience means to minimize the advent of business disruption in the face of cyberattacks in the context of a strong security posture.

Cyber resilience has traditionally been considered from the perspective of governments, private sector companies, and organizations, although the impacts of adverse cyber events on individuals is now evident. The common way it is perceived reflects the potential harmful consequences on machines, computer, and technical systems. However, this perspective fails to reflect the very multi-dimensionality of cyber resilience, considering the role and the responsibilities of the civil society stakeholders in guaranteeing an adequate level of cyber resilience. Cyber resilience should be considered as a future right of individuals within the whole society.

For developing a cyber-resilience aware society, it is needed the involvement of civil society stakeholders in the development of cybersecurity strategies starting from the analysis of the extent to which resilience is incorporated into the countries' cybersecurity strategies. Furthermore, the roles, responsi-

bilities, and modalities of participation of the civil society stakeholders (i.e., individual citizens, communities, and third-sector organizations) in the strategies must be properly defined.

AI impact on a cyber-resilient industry

In this section, we will discuss the use of AI in the cybersecurity and the context of cyber-resilient industry. The main aspect of the AI that meet interest in this application is related to the use of machine learning and in particular deep learning in the various aspects like convolutional approaches, generative models and the novel frontier of meta learning models. In cybersecurity, AI-based tools and methodologies can help to prevent sophisticated attacks by learning the behavior of attackers.

Vulnerability management: strategies and processes

Vulnerability management (VM) can be defined as an ongoing process of identifying, assessing, reporting on, managing and remediating cyber-vulnerabilities across endpoints, workloads, and systems. The main approach to VM can be to have a security team that will design a vulnerability management tool to detect vulnerabilities or exploit an existing one. VM also include the definition of suitable processes to patch or remediate the detected vulnerabilities.

To improve VM programs, AI can be used to highlight and prioritize threats and risks thus addressing vulnerabilities in real time.

A vulnerability, as defined by the International Organization for Standardization (ISO 27002) is a weakness of an asset or a mix of assets that can be exploited by one or more threats. A threat is something that can exploit a vulnerability. A risk is what happens when a threat exploits a vulnerability. It's the damage that could be caused by the open vulnerability being exploited by a threat.

An attack could be generated by exploiting one or more vulnerabilities. Different kinds of attacks exist and can involve several assets in an organiza-

tion by generating a consequence in terms of availability (e.g., DoS or DdoS can cause an interruption of IT services), confidentiality (e.g., information stolen without the knowledge or authorization of the system's owner causing a data breach), or data integrity (e.g., malware or spyware able to corrupt or delete data). These consequences can impact company productivity, damage to image, possible loss of customers, and economic damage.

Therefore, the scope of VM is to minimize the attack surface: any weak point in digital assets belonging to an organization that a possible attacker can gain access to. It is worth noting that considering the specific domains of the organization, these weaknesses can be related to IT/OT/IoT systems and assets.

Indeed, the first step related to this process involves assets' discovery and prioritization. This phase aims to create a total assets inventory across the organization. Then, the assets should be classified, prioritizing the business-critical ones based on impact and risks; this classification will help in understanding priorities or driving decisions when is evaluated the strategy of the VM processes. Finally, in this phase, key performance indicators (KPI) should be identified to report progress and measure the success of your vulnerability management program.

At this point, vulnerability scanning should be performed by an adequate vulnerability scanner able to identify vulnerabilities across the assets in a continuous and automated way. Once vulnerabilities have been identified, they must be rated and organized by risk and appropriate KPIs defined by also the organization's risk assessment processes.

The following step regards addressing the vulnerabilities. Several strategies can be considered:

- Remediate the vulnerability by fully fixing or patching it.
- Mitigate the vulnerability by minimizing the potential damage or decreasing the possibility of its exploitation.

- Where the risk is low accept the risk of the vulnerability and take no action.

Once vulnerabilities are remediated or addressed, it is fundamental to report vulnerabilities solved and known. Indeed, in the VM process, regular internal follow-ups are necessary to ensure that threats have been eliminated.

This cyclic process should be continuous in any organization and improved step by step by the regular scanning of assets that allows more and more comprehensive awareness of the organization's weaknesses and remediation plans.

Deep and Meta learning solutions for vulnerability management

The usefulness of AI models in the field of cybersecurity and, more generally, of the security of information networks is a basically related to the possibility of introducing models that are safe transparent and efficient. This is possible using X-AI, namely explainable AI.

It is evident that justify the models' decisions and possibly detect and explain the reasons of errors can improve the reliability and the trustworthiness of models based on AI. Furthermore, the possibility of interpreting models' behavior allows to better adhere to regulations and protection of personal information, thus improving transparency of the procedures.

The main areas of information security can be resumed as: 1) intrusion prevention and detection; 2) access control and authentication; 3) privacy, trust, and reputation.

Indeed, there are many causes of vulnerabilities, such as the growing need for devices' connection that exposes most of the applications and interfaces, also when is not necessary or not managed, to the internet (1); the increasing complexity of systems that require ever and ever punctual management of ac-

cess control policies and authentication methods (2); poor password management policies leading to possible data breaches (3). Also, people in the organization can be the driver of vulnerabilities because they can become victims of social engineering attacks jeopardizing the company's assets (3).

The above-mentioned situations can be avoided or mitigated by implementing efficient protections such as adopting Intrusion Detection System or/and Intrusion Prevention System to identify suspicious network activity by analyzing and monitoring traffic and discovering unusual elements or activities. These systems can discover outdated or unpatched software and hardware; malware; attack vectors. Furthermore, it is worth noting that a consistent part of discovered vulnerabilities is reputable to old versions of software that need to be upgraded or dismissed. Indeed, the first recommendation is maintaining an up-to-date version of IT components.

Finding new ways to automate and improve the discovering of these flaws in IT environments is becoming ever and ever important. Actually, security analytics can take advantage of ML and human-based AI to deliver improved outcomes.

Most of the present AI techniques can be useful to modern vulnerability management systems in many ways, e.g., to develop an in-depth understanding of the context of each asset. When the asset's context is acquired, it can be combined with some knowledge of the specific vulnerability and the external threat environment to generate a "context-driven priority." An intelligent vulnerability management program can allow us establishing priorities and to define a plan for risk reduction by optimizing scarce remediation resources, thus through a context-sensitive assessment of risk.

AI-based sentiment analysis is widely used by brand marketing professionals to assess posts on social platforms and media to reference their products. AI can be considered as a good potential tool for inferring how a brand is perceived and how this perception is evolving over time: this can be carried

out by collecting related data. Cybersecurity chat boards, and other online sources of cybersecurity conversations can be analyzed to predict which vulnerabilities are the most likely to be exploited, which security experts are most concerned about, and how those sentiments change over time.

This kind of analytics becomes impractical for humans as the number of information available is huge and is growing continuously: AI tools, like neural DL, can be appropriately used with Natural Language Processing (NLP) techniques to extract meaning and the level of threats in addition to technical information from text. AI and DL can help to interpret many posts and blend their meanings to add context to any given vulnerability's practical risk, considering that the community of participant actors is ever-growing in the media.

It is evident that in such context, the availability of tools that can help interpret or explain the decisions of a DL/AI system can make the difference. Marketing managers can plan the product evolution, and cybersecurity professionals can delineate the strategy for reducing risks of cyberattacks by exploiting such automatic suggestions.

Conclusions

In this paper, we analyzed the impact of a cyber-resilient industry on our society. We reported the process of vulnerability management related to the most common exploited strategies and processes. Then, we investigated how Deep and Meta learning solutions can improve vulnerability management systems and make the results of such systems more accessible and useful for the organization's needs. In the future, we plan to propose a solution able to integrate such features to a chosen vulnerability management system.

References

1.https://cs.unu.edu/smart-citizens-cyber-resilience/national-cyber-security-strategies-review

2.https://cs.unu.edu/smart-citizens-cyber-resilience/capacity-building

3.https://www.cisecurity.org/wp-content/uploads/2018/07/Cybersecurity-Tech-Basics-Vulnerability-Management-Overview.pdf

4.https://www.techtarget.com/searchsecurity/tip/How-to-build-a-better-vulnerability-management-program

5.Kaur, Ramanpreet, Dušan Gabrijelčič, and Tomaž Klobučar. "Artificial intelligence for cybersecurity: Literature review and future research directions." Information Fusion (2023): 101804.

6.de Azambuja, Antonio João Gonçalves, et al. "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey." Electronics 12.8 (2023): 1920.

7.Bonfanti, Matteo E. "Artificial intelligence and the offence-defence balance in cyber security." Cyber Security: Socio-Technological Uncertainty and Political Fragmentation. London: Routledge (2022): 64-79.

8.Aslan, Ömer, et al. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions." Electronics 12.6 (2023): 1333.

9.Syed, Romilla. "Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system." Information & Management 57.6 (2020): 103334.

10. Mohammed, Ishaq Azhar. "Artificial intelligence for cybersecurity: A systematic mapping of literature." ARTIFICIAL INTELLIGENCE 7.9 (2020).

FINANZAS SOSTENIBLES EN LA ERA DEL ARGOCAPITALISMO: EL PAPEL DE LA CIBERRESILIENCIA

Dr. Enrique López González
Académico de Número de la Real Academia de Ciencias Económicas y Financieras

¿Acaso son válidas hoy en día estas tres aseveraciones:

"El defecto habitual del hombre es no prever la tormenta cuando hace buen tiempo".
Nicolás Maquiavelo

"Sabemos por la historia que simplemente no tenemos la imaginación para anticipar adónde nos pueden llevar las nuevas tecnologías de la información".
John Preskill

"Una onza de prevención vale más que una libra de cura".
Benjamin Franklin

Distinguido auditorio, les prevengo que las palabras que siguen a continuación se inspiran en tales premisas, eso sí, referidas a las finanzas en este cambio de época actual.

No parece necesario disponer de un alto grado de experticia para aseverar que las finanzas son la sangre, el elemento vital, de las economías en crecimiento. Fluye por las arterias del tráfico comercial, alimentando la innovación de las empresas, contribuyendo decisivamente a convertir grandes ideas en negocios prósperos.

A mayores, con el advenimiento de la Sociedad 5.0, basada en el sincretismo tecnológico de la ecologización y digitalización de la economía cuya simbiosis propicia nuevos tiempos de auténtica mutación tecnológica, las finanzas se han vuelto particularmente críticas, como se pretende demostrar en esta necesariamente sucinta disertación.

En primer término, respecto a la ecologización de la economía, cabe observar cómo toda Europa, y gran parte de los países desarrollados, está en una cruzada contra el calentamiento global para que en los próximos 27 años puedan convertirse, al menos, en economías de cero emisiones netas al mismo tiempo que tenemos que revertir el declive de la naturaleza y adaptarnos y mitigar en lo posible los efectos del sobrecalentamiento global. Además, en este mismo momento, cuando hace ya más de un año de la invasión ilegal de Rusia en Ucrania, también debemos protegernos de los mercados energéticos internacionales volátiles resultantes de la deleznable decisión de Putin.

Con todo, cabe avizorar que las recompensas ambientales y económicas de esta transformación posiblemente serán inmensas, pero los desafíos involucrados no son menores, a saber: No solo se precisan empresas pioneras y emprendedores para crear productos y servicios ecológicos, también es necesario disponer de una estructura de apoyo adecuada para impulsarlos hacia el éxito de prosperidad compartida.

De ahí que las Nuevas Finanzas sean tan cruciales en la carrera por financiar la Revolución Verde (y Digital) que conlleva la Sociedad 5.0, pues nuestra capacidad para explotar sus oportunidades dependerá de nuestra disposición a financiarla.

Hablamos entonces de Nuevas Finanzas, pues, en Europa y particularmente en España, para poder desfosilizarnos (finiquitar la combustión como base energética) en 27 años y así cumplir los objetivos ambientales a la par de brindar seguridad energética, necesitaremos un cambio radical en los niveles de inversión.

En efecto, la transición global hacia una economía neta cero, positiva para la naturaleza y resiliente exigirá que billones de euros se reasignen e inviertan en nuevas tecnologías, servicios e infraestructura que puedan abordar los riesgos del cambio climático y la degradación ambiental. La sostenibilidad es una obligación tanto práctica como moral.

Desde eventos climáticos cada vez más frecuentes y severos que causan daños a la infraestructura y las cadenas de suministro, hasta cambios en las expectativas y preferencias de los consumidores que modifican la demanda de ciertos productos y servicios, las empresas y sus inversores necesitan contar con las políticas adecuadas para ayudarlos a administrar estos riesgos y evitar activos bloqueados.

Actuar ahora también es importante para minimizar los riesgos fiscales de la transición y maximizar las oportunidades de crecimiento: los costes de la inacción son tan significativamente altos que dejan de ser una opción para convertir la adaptación y mitigación en un imperativo. Como la naturaleza sustenta las economías y los medios de subsistencia, y como proteger y restaurar la naturaleza es inseparable de abordar el cambio climático, por ende, se precisa incorporar tanto la naturaleza como la adaptación climática en las nuevas finanzas.

A este respecto participamos de la opinión del Profesor Stiglitz, Nobel de Economía y miembro de nuestra Real Corporación, cuando califica a la crisis climática como "*nuestra tercera guerra mundial que precisa de una respuesta audaz: pagaremos por el cambio climático de una forma u otra, por lo que tiene sentido gastar dinero ahora para reducir las emisiones en lugar de esperar hasta más tarde para pagar mucho más por las consecuencias. No hay absolutamente ninguna razón para que la economía innovadora y verde del siglo XXI tenga que seguir los modelos económicos y sociales de la economía manufacturera del siglo XX basada en combustibles fósiles, así como no había ninguna razón para que esa economía tuviera que seguir los modelos económicos y sociales modelos de las economías agrarias y rurales de siglos anteriores"*.

El futuro es ahora y este es el momento de impulsar la transición, aprovechar esta oportunidad, mitigar esos riesgos y garantizar los flujos financieros necesarios para comercializar y financiar las tecnologías verdes necesarias para la transición, para ofrecer fuentes de energía renovables, baratas y lim-

pias para calentar nuestros hogares, enfriar nuestros refrescos, movilizar nuestro transporte, a la par de impulsar nuestras industrias de cero neto, seguridad energética y amigable con el medio ambiente.

De cumplirse tales previsiones, cabe argumentar que entonces Europa podrá utilizar su liderazgo y la experiencia de su sector financiero para acelerar el cambio hacia un sistema financiero global verde y catalizar el financiamiento verde a nivel mundial. De esta forma en este tiempo cercano se podrán ver los mayores cambios en la industria desde el siglo XIX, a medida que pasamos de una economía impulsada por combustibles fósiles a una desfosilizada, donde podremos legar nuestro medio ambiente en un estado mejor de lo que lo encontramos.

No extraña entonces como en la actualidad, existe un amplio consenso en estructurar la idea de sostenibilidad en torno a tres conceptos fundamentales que conforman las siglas de ASG. Nos referimos a los aspectos Ambientales, Sociales y de Gobernanza. De este modo, las finanzas sostenibles se refieren a cualquier forma de servicio financiero que integre criterios ASG en las decisiones de negocio o de inversión.

Esta nueva forma de enfocar las finanzas supone un cambio radical de cultura, que, poco a poco, se está adaptando para satisfacer las demandas de un público (reguladores, supervisores, analistas, accionistas, clientes, etc.) cada vez más concienciado.

No obstante, también resulta común que algunas empresas hagan afirmaciones exageradas o engañosas relacionadas con la sostenibilidad sobre sus productos de inversión; afirmaciones que no resisten el escrutinio (lavado verde).

Esto puede provocar daños al consumidor y erosionar la confianza en el mercado de productos de inversión sostenible, de ahí la importancia por la existencia de una contabilidad que resalte el valor de la información ASG

para capturar las dimensiones clave de una sustentabilidad más amplia; es decir, cómo las personas, el planeta, la prosperidad y el propósito se unen para ayudar a permitir que "las necesidades del presente [se satisfagan] sin comprometer la capacidad de las generaciones futuras para satisfacer sus propias necesidades" (en línea con el informe "Nuestro Futuro Común" de las Naciones Unidas [1]).

Además del impacto de que la economía se ecologice, el segundo aspecto a considerar en esta presentación se refiere a la digitalización de la economía, entendida, en términos no acordes con la Real Academia Española [2], como la continua convergencia de lo real y el mundo virtual, esto es, que la mayoría de nuestras actividades diarias dependen en gran medida de tecnologías digitales innovadoras. De hecho, la digitalización es la integración de las tecnologías digitales en la vida cotidiana.

En la episteme actual está generalizado que la digitalización constituye la fuerza prístina impulsora de la innovación y la radical mudanza acontecida en la economía política en este inicio de Siglo XXI pues, tiene el potencial de

1 "Report of the World Commission on Environment and Development

2 Lamentablemente nuestro Diccionario de la Real Academia Española (RAE) registra la palabra digitalización como «acción y efecto de digitalizar» y, a su vez, la palabra digitalizar como «1. registrar datos en forma digital y 2. convertir o codificar en números dígitos datos o informaciones de carácter continuo, como una imagen fotográfica, un documento o un libro». Por el contrario, cabe observar que el Diccionario Inglés de Oxford (OED) si difiere explícitamente, dado el valor analítico fundamental que tal distinción conlleva, los términos "digitization" y "digitalización". En el OED, la "digitization" hace referencia a "la acción o el proceso de "digitizing": "la conversión de datos analógicos (ya sean imágenes, vídeo o texto) en forma digital". "Digitalization", por el contrario, se refiere a "la adopción o el aumento en el uso de la tecnología digital o el ordenador por una organización, la industria, el país, etc.". Dos letras marcan una diferencia sustancial. La digitalización va más allá de la digitización, al aprovechar la tecnología de información digital para transformar por completo los procesos de un negocio o actividad: evaluar y reimaginar la forma en que se genera valor. Así, la digitización es una conversión de datos y procesos, la digitalización es una transformación, el proceso de pasar a un negocio o actividad digital. La digitalización, además de digitizar los datos existentes, abarca la capacidad de la tecnología digital para recopilar datos, establecer tendencias y tomar mejores decisiones. Así, por ejemplo, un documento se puede digitizar mientras que una fábrica se puede digitalizar.

transmutar radicalmente la ciencia, la sociedad o la economía donde, cada vez más, las instituciones son sustituidas por la negociación algorítmica. Esta ola continua de transformación tecnológica crea abundantes oportunidades, pero también considerables desafíos que deben superarse a lo largo del proceso de su implantación y desarrollo.

La digitalización no se limita a los aspectos técnicos, sino que repercute en todos los ámbitos sociales y socioeconómicos, planteando la emergencia de un nuevo orden económico, que me he atrevido a denominar "Argocapitalismo" (López-González, 2020) [3], entendido como toda la serie de cambios culturales, laborales y de tecnología profundos y coordinados que permiten nuevos modelos operativos basados en datos que transforman las operaciones, la dirección estratégica y la propuesta de valor meta-personalizada de una institución.

En el Argocapitalismo, los datos [4], las auténticas células de la economía digital son una forma de capital, de igual nivel que el capital económico o el financiero, en términos de generar nuevos productos y servicios digitales. De hecho, si bien en la actualidad se acepta que los algoritmos son uno de

3 El basamento etimológico del prefijo "argo-" como calificativo de este "nuevo capitalismo", se apoya en un epónimo dual, pues, como en las monedas, cabe considerar dos caras o perspectivas: Por un lado, la cara, predictiva o anticipadora de comportamientos a través del manejo de datos, que está inspirada en el mito griego de Jasón y los argonautas que navegaron a la búsqueda del vellocino de oro en "la Argo", la fabulosa nave pentecóntera cuya proa, construida con madera de Dodona, tenía el don del habla y de la profecía. Y, por otro, la cruz, panóptica o de vigilancia, vinculada a la extracción de datos, que se inspira en el mito griego de Argos Panoptes, "el que todo lo ve", cuya fabula quedo retratada magistralmente por Velázquez en su magnífico lienzo "*Mercurio y Argos*" del Museo del Prado (https://www.museodelprado.es/coleccion/obra-de-arte/mercurio-y-argos/d15f630f-cc1c-42c4-80e6-14087dfcecb5)

4 En el diccionario de la RAE, se recogen 3 entradas de la palabra *dato* (del latín *datum* 'lo que se da'): (1) Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho, (2) Documento, testimonio, fundamento y (3) Información dispuesta de manera adecuada para su tratamiento por una computadora. También, se contemplan 2 entradas del verbo *datear*: (1) Dar alguna información o dato a alguien y (2) Entregar datos confidenciales para que puedan ser utilizados para obtener un beneficio personal.

los principales motores de la vida económica y social, entonces resulta fácil convenir en que los datos son el combustible, la electricidad, que los hace funcionar.

Por tanto, bajo la nueva lógica formal del capitalismo, el valor se encuentra en los datos, siendo la recopilación y circulación de datos el elemento central que lo caracteriza, la nueva ecuación que conlleva la transformación digital del sistema económico: Los datos son el capital.

Entender los datos como una forma de capital propicia poder analizar mejor el significado, las prácticas y las implicaciones del régimen político económico derivado de la digitalización, esto es, la naturaleza y la dinámica del argocapitalismo.

Así, en lugar de que la recolección de datos sea vista simplemente como una forma de producir materias primas que de alguna manera se convierten en valor monetario, la "dateación" se configura como un régimen político económico impulsado por la lógica de la acumulación y circulación perpetua de capital. Precisamente, aquí es donde radica una de las ideas centrales que inspiran a los argocapitalistas: sea cual sea el producto que se fabrique o servicio que se preste en la actualidad, conviene examinarlo como una proporción de átomos a bits.

La cuestión que se plantean es sencilla: ¿Hay una manera de digitalizar la información que la cosa lleva y entregarla como un servicio a través de un teléfono inteligente o dispositivo conectado? Y así, los argocapitalistas, "fanáticos de los datos", se enfocan con denuedo en "ver los datos que no estaban allí" e imaginar nuevas formas de capturarlos y usarlos.

Conviene observar entonces que tanto los datos como la digitalización se han convertido en un arma de doble filo. Son impulsores clave de valor y eficiencia, pero también crean un nuevo producto objetivo importante y una mayor vulnerabilidad corporativa, esto es, la superficie de ataque continúa

creciendo, y defenderse contra las infracciones no es suficiente cuando los datos, la infraestructura digital y las aplicaciones se trasladan al centro de los negocios y la sociedad, como claramente lo han estado haciendo.

Además, la naturaleza de los riesgos cibernéticos cambia con los ataques y las infracciones que a menudo tienen consecuencias de gran impacto. Nos guste o no: estamos en un punto de inflexión y necesitamos un enfoque más holístico y estratégico que ofrece la resiliencia cibernética o ciberresiliencia.

Todavía, hoy en día, la toma de decisiones en la gestión de emergencias y la respuesta a crisis está impulsada por teorías, modelos y herramientas establecidos de evaluación y gestión de riesgos.

La evaluación de riesgos requiere una identificación de amenazas, vulnerabilidades y consecuencias con ciertos supuestos y en escenarios operativos específicos que pueden dar como resultado una capacidad de predicción limitada y un soporte de decisiones poco confiable. Dado que las amenazas sistémicas son en gran medida inciertas e impredecibles, la cuantificación de amenazas es difícil y la asignación conservadora de probabilidades más altas a escenarios de amenazas poco frecuentes puede dar lugar a soluciones de gestión de riesgos que son prohibitivamente costosas.

Además, la mayor complejidad de la convergencia actual del mundo humano-ciber-físico plantea nuevos desafíos. Los seres humanos están profundamente inmersos en los flujos de información bidireccionales, lo que hace que nuestra sociedad sea aún más vulnerable a nuevas formas de amenazas que explotan la mayor superficie de ataque que ofrecen las profundas interdependencias existentes en estos sistemas humanos-ciber-físicos.

Para rizar más la situación, otro efecto de la complejidad es la presencia de problemas no repetitivos (que requieren decisiones no repetitivas) y problemas no estructurados que son difíciles de predecir (es decir, los cisnes ne-

gros de Taleb) o cuantificar el impacto, lo que dificulta precisar los objetivos tangibles que una solución debe lograr. Incluso, la existencia de múltiples y diversos subsistemas con interacciones complejas, no lineales y a veces ocultas, combinadas con las amenazas nuevas y emergentes, requiere enfoques capaces de hacer frente a "incógnitas desconocidas", así como a múltiples dimensiones y escalas de análisis y acciones.

De ahí que, en esta era del argocapitalismo, un mundo vuca, en red y siempre conectado, contar con nuevos paradigmas y tecnologías para hacer frente a los factores estresantes tan complejos sea una necesidad primordial e improrrogable.

Hoy en día, los recursos se gastan principalmente en medidas de mitigación de riesgos que apuntan a prevenir o minimizar los impactos de riesgos específicamente conocidos. Sin embargo, dada la considerable interrupción que tales amenazas sistémicas pueden representar, las organizaciones, ya sean privadas o públicas, deben pasar de un enfoque basado en amenazas a uno basado en la resiliencia, a fin de respaldar la toma de decisiones para mantener las actividades económicas, su funcionamiento, en presencia de riesgos nuevos/no anticipados con impactos compuestos y fallas en cascada resultantes. Por tanto, pasando de centrarse en los riesgos a centrarse en sobrevivir y esforzarse en la recuperación.

Pero, la resiliencia es más que la capacidad de recuperarse rápidamente, la resiliencia significa lidiar con la adversidad y los impactos, y adaptarse continuamente para crecer. Las organizaciones verdaderamente resilientes no solo se recuperan mejor, en realidad prosperan en ambientes hostiles, no solo superan a sus pares durante una recesión y recuperación, sino que también se aceleran hacia la nueva realidad, dejando a sus pares más atrás. Al enfrentarse a un mundo de interrupciones continuas y superpuestas, tales organizaciones están reconociendo la resiliencia como la condición imperativa para asegurar un futuro sostenible e inclusivo.

Pensar en la resiliencia de esta forma obliga automáticamente a las organizaciones a incorporar factores ASG en sus funciones de gestión de riesgos. Cuando se integran correctamente, los factores ASG con la ciberresiliencia, pueden dar a las organizaciones las señales correctas sobre el riesgo y el cambio.

Vale

ECONOMÍA Y CIBERDELINCUENCIA CUÁNTICA

Dr. José Daniel Barquero
Académico de Número de la Real Academia de Ciencias Económicas y Financieras

La ciberdelincuencia es un acto delictivo perpetrado a través de internet y de las nuevas tecnologías de la información y de la telecomunicación.

Siendo a través de estos actos, el que los ciberdelincuentes, puedan robar dinero con la estafa y el chantaje, además de atacar causando daños irreparables a empresas e instituciones, así como a personas, redes, colectivos, webs e incluso países.

Dependiendo de la envergadura de los actos delictivos, se podría incluso llegar a desestabilizar y vulnerar la seguridad de los usuarios y afectar incluso a la buena marcha de las organizaciones y de la economía de un país.

Pero mientras la ciencia en cuanto a computación cuántica e inteligencia artificial se refiere avanza a una hipervelocidad sin límites en todo el mundo, (con EEUU y China a la cabeza), la Unión Europea, se propone empezar a legislar sobre la misma.

La legislación actual sobre los problemas propios que se desprenden de la inteligencia artificial es prácticamente inexistente. El principal problema al tratar de legislar algo tan moderno y que adelanta tan rápido su investigación es que cuando llega el momento de hacerlo el objeto de la legislación ha quedado obsoleto y en consecuencia al ser un tema que atañe al mundo es necesario unificar criterios de actuación.

El pasado jueves día 11 de mayo de 2023 nos despertábamos con noticias en las redes conforme a que se aprobaba el nuevo reglamento por parte del

Parlamento Europeo del que destacamos que no permitirá a esta ciencia espiar, se tendrán además en cuenta, los derechos de autor, vetarán sistemas de categorización biométrica en cuanto a sexo, raza, religión, etnia y otros como los capaces de detectar individuos por reconocimiento facial, todo un reto.

Todo gira en torno a la ciencia como académicos lo sabemos es imparable y si se regula en Europa y se liberaliza en países como China, Japón, EEUU y otros muchos, hasta 180 nos podemos encontrar que nos tomen la delantera. De entrada, Bard el asistente de inteligencia artificial de Google ya está disponible en esos 180 países, pero no en Europa, siendo capaz Bard entre otras cosas de responder a cualquier pregunta ampliamente a la vez que permite corregir fácilmente y rápido nuestras fotos, así como nuestras cartas y escritos de todo tipo, dándoles más realce y si hablamos de rutas nos las ofrecerá en un 3D muy mejorado. Lo mismo ocurrirá con muchas otras aplicaciones y adelantos científicos ya que esto, puede dar paso a ciberdelincuentes de fuera de la Unión Europea y que delincan en nuestros países con tecnologías liberadas en esos 180 países, teniendo en Europa presas fáciles que abordar.

Pero ¿Qué pasará con los ciberdelincuentes cuánticos? ¿Realmente los ordenadores cuánticos revolucionarán la ciencia y el planeta en su totalidad?

¿La computación cuántica acabará con la ciberdelincuencia o la potenciará?

¿Es peligrosa para el planeta o realmente es la solución? ¿La cuántica es la solución a todos los problemas que pueda plantearse la empresa y la economía mundial? ¿La cuántica resolverá donde invertir y dónde no con garantías de éxito?

Para dar respuesta a estas preguntas a las que llegamos tras una investigación de mercado, a 50 ejecutivos de empresas líderes en sus respectivos sectores, empezaremos definiendo que es un ordenador cuántico. Ya que este, utiliza la mecánica cuántica, para procesar datos de tal forma que sus cálculos

son los más precisos, eficientes, rápidos y seguros gracias a los cúbits (bits cuánticos) que a diferencia de los bits (dígitos binarios) utilizados hasta ahora, cambiarán el curso de la economía y de la sociedad en la que desarrollamos nuestras actividades.

Siendo los cúbits los que contienen más información y capacidad de acierto y la facilitan de forma extremadamente más rápida, es más son de naturaleza extremadamente probabilística y los bits son de naturaleza determinista.

El ordenador cuántico de cúbits permite en minutos hacer cálculos que con un ordenador de bits (los actuales ordenadores), tardaríamos cientos de años en resolver.

Hace tan solo unos meses en un encuentro académico de esta Real Corporación en la Universidad de Salamanca y presidido por el Presidente de esta Real Corporación el Catedrático y DR JAIME GIL ALUJA, llegamos a la conclusión, de que la computación cuántica que se avecina, cambiará la economía, hacia una nueva economía que girará en torno a lo cuántico y que está, estaba más próxima a la física cuántica en cuanto a probabilidades se refería.

En esta competición por liderar la ciencia cuántica y los cúbits han sido noticia empresas líderes como: Baidu, IBM,Google, siendo esta última quien hace dos años anunció la supremacía cuántica incluso antes de que lo pronunciaran los científicos chinos. Tal es así que la capacidad de los cúbits permite resolver los problemas económicos más complejos que puedan existir en el mundo y no equivocarse en inversiones económicas y financieras, detectando falsas expectativas que tenga dicha inversión, por mucho que se invierta por parte de las compañías en darles más empaque con grandes gurús del mk, del lobby o de las relaciones públicas.

Siendo muchas las startup y empresas que se verán abocadas al cierre, pues la nueva economía cuántica será capaz de advertir al inversor del peligro

que corre si hace una inversión o bien de que no la lleve a cabo o bien de que salga urgentemente de dicha inversión o por contra que continúe con esta. Pero ¿Qué pasará con las empresas que los ordenadores cuánticos recomienden invertir?, pues que el precio de estas acciones como apuntaba en nuestro congreso de Belgrado el Académico DR MARIO AGUER empezará a subir, aumentando el precio de la acción. Esto puede llevarnos a que incluso llegue a valer más la propia empresa de lo que ésta pueda generar por las expectativas reales de beneficio que sin duda dictará la economía cuántica y la inteligencia cuántica y que a los pocos días corregirá su propia opinión para decirnos que vendamos que las acciones están súper inflacionadas. Como decía nuestro académico el Magistrado ENRIQUE LECUMBERRI, en el último acto de esta academia, será un mundo de acción y reacción, rápida a tiempo y en el momento oportuno.

La nueva economía cuántica, será liderada por la información que se desprenda de estos potentes ordenadores y ya no existirán buenos o malos economistas existirán ordenadores cuánticos o no, los cuales facilitarán la inversión y la toma de decisiones. En consecuencia, ya no se tratará de facturar más cada año a cualquier precio en las empresas, sino que no cueste más, el hecho de facturar más, que los propios beneficios de la empresa y la computación cuántica lo delatará rápidamente poniendo en aprietos a muchas compañías. Ya incluso no mandará la auditoría de cuentas, mandará la computación cuántica.

Ocurre que existen muy reconocidas startup y empresas hoy en día que pierden dinero por cada servicio a su cliente y que independientemente lo siguen llevando a cabo sin problemas, porque aumentan la facturación no así los beneficios, pero no se sabe lo suficiente, con la computación cuántica se sabrá en el mismo momento que ocurra, advirtiendo al inversor. Si bien, aunque aumenten los costes, como aumentan la facturación ocurre que el precio de la empresa por las expectativas de esta facturación crece de valor en el mercado. Un ejemplo parecido lo tenemos en Glovo que según sus cuentas públicas desde el 1 de enero del 2022 sus ventas fueron de 590 millones de euros sin embargo sus pérdidas fueron de 474 millones de euros.

La hipervelocidad que está adquiriendo la inteligencia artificial que nos argumenta el académico Dr. ENRIQUE LÓPEZ unido a la computación cuántica y a su vez aplicado a la economía hace que las instituciones económicas y financieras de los países más avanzados inviertan potentes cantidades de dinero esperando es justo reconocer pingües beneficios y seguridad en todas sus transacciones.

El procesador cuántico más moderno es Osprey, patentado por la reputada IBM, el cual dispone de más de 400 cubits, pero esta empresa prepara un nuevo chip con el que cambiarán el mundo y que contendrá más de 1.100 cubits.

Lo anteriormente expuesto hace que nos preguntemos ¿Qué ocurrirá con la ciberdelincuencia cuántica? La respuesta es relativamente fácil se reduce su respuesta a la adaptabilidad al cambio en consecuencia los ladrones, delincuentes y estafadores profesionales a día de hoy evolucionan con el tiempo y las nuevas tecnologías y son los que operan en internet, siendo conocidos bajo el sobrenombre de ciberdelincuentes o incluso cibercriminales. Su modus operandi ha evolucionado ya que algunos empiezan estafando en su ciudad, para luego hacerlo en ciudades vecinas, adaptando la misma a las costumbres del país y con las facilidades de los nuevos y potentes traductores, el traducir sus estafas a varias lenguas y delinquir con sus estafas en todo el mundo. Pero con la tecnología cuántica aplicada a la ciberdelincuencia si se utiliza bien estos delincuentes verán muy reducidas sus formas de estafar pues permitirá detectar intrusos en los sistemas, avisará de las estafas rápidamente y un largo etc. No obstante, si se utiliza mal la computación cuántica el peligro está garantizado y si otros países no legislan y Europa si, podemos ser receptores de peligrosos estafadores cuánticos.

En la actualidad este tipo de crímenes cibernéticos sustraen en todo el mundo la cantidad de más de 600.000 millones de dólares, según un estudio realizado por McAfee empresa líder en la creación de antivirus y el CSIS Centro de Estudios Estratégicos Internacionales. ¿Cuánto podrá llegar a sustraer los ordenadores cuánticos? Todo, pues deja obsoleto nuestro sistema actual de seguridad.

La inquietud en cuanto a lo sustraído es tal que es necesario que veamos algunos ejemplos de estos ciberdelincuentes y el daño que pueden llegar a ocasionar hoy en día y antes de que llegue la temida ciberdelincuencia cuántica:

Kevin Mitnick, en un alarde de demostrar lo que era capaz de hacer, llegó a robar datos muy importantes del comando de defensa de los EEUU, así como los datos de la Digital Equipment Corporation, para a continuación ser detenido y desde la propia prisión atacar los sistemas de la Pacific Bell Telephone Company.

Michael Calce, con sus actos delictivos en las redes y con tan solo 17 años hizo que los EEUU incluso cambiaran su legislación vigente. Siendo Michel el ciber delincuente capaz de modificar resultados de Yahoo así como adquirir el control de cuanto le placía en distintas universidades. Incluso llegó a bloquear empresas gigantes dejándolas fuera de juego con ataques a eBay, Amazon, CNN y otras muchas.

Kevin Poulsen, su ciberdelincuencia le llevó con tan solo 17 años a introducirse en los sistemas de seguridad más complejos de los EEUU en el Pentágono y para demostrar su osadía hasta publicar los datos secretos del propio Pentágono referentes a Filipinas. En la actualidad es asiduo escritor de la revista Norteamericana Wired dedicada a demostrar el impacto de las nuevas tecnologías en la sociedad mundial.

El Grupo Astra, del que se desconoce quién está detrás llegó a introducirse en el grupo Dassault y piratear su potente software tecnológico, así como la información confidencial sobre sus armas de gran tecnología.

Alberto Gonzalez , este ciberdelincuente cubano afincado en EEUU fue capaz de robar desde la red 170 millones de tarjetas de crédito, así como números secretos de cajeros automáticos. Fue acusado por tres acusaciones federales y condenado a 20 años de prisión.

Annnonymous y OuerMine corresponden a las dos organizaciones ciberdelincuentes más peligrosas de Hackeo quienes chantajean a sus víctimas robando perfiles e inhabilitando webs.

El Cóndor, es un alias de Kevin Mitnick quien fue el que hackeó los sistemas de Motorola y Nokia y hoy es consultor en ciberdelincuencia.

Popescu, se especializó en subastas de coches y otros artículos de lujo que además no existían, se trataba solo de fotos robadas de otros sitios web o trucadas en las webs de las subastas más importantes de internet,.

Vladimir Levin, fue el autor cibernético del robo de 10 millones de dólares al Citibank.

Crackca, fue capaz de introducirse en la CIA y publicar la identidad de más de 30.000 agentes en las redes.

Todos estos crímenes quedarán en crímenes ridículos y podrán ser evitados con la computación cuántica, pero quien controle dicha computación tendrá también el poder de hacer el mal y en consecuencia robar lo que se le antoje y ahí radica el peligro de la nobleza del primer país que la disponga que esperemos su lema sea el de paz y bien.

En los EEUU, la Nasa ya en el año 2.014 tomó una importante decisión e invirtió pioneramente más de 80 millones de euros en investigar la computación cuántica.

De ahí que Europa se diera cuenta de su importancia y después de ese momento que marcó un antes y un después se decidiese a invertir en tecnología cuántica la cifra de 4.500 millones de euros, desde este año 2.023 al 2.027. Nuestro país vecino, Francia en 2.021 decidió invertir en computación cuántica la cifra de 1.800 millones de euros y así varios países.

Pero esto hace que nos preguntemos: ¿Cuál es el objetivo de estos países? Pues entre otros, obtener la hegemonía mundial por ejemplo en salud sería capaz de crear medicamentos eficaces para curar el cáncer. En cuanto a seguridad evitar el fraude bancario o anular la ciberdelincuencia a nivel mundial, pero mal utilizado permitiría también el espionaje aplicado a países y a industrias.

Por si fuera poco, el primer país en tenerlo tendría en sus manos la desestabilización mundial pues dispondría de las claves de cifrado asimétrico o lo que es lo mismo el poder hacer una tercera guerra mundial cibernética pues decidirán si hacen un apagón mundial pudiendo colapsar a su antojo todos los sistemas de información.

La BBC publicaba un artículo que adquirió un gran realce internacional titulado "Apocalipsis Cuántico" es decir en el que afirmaba que todos los sistemas de seguridad e información de las empresas y gobiernos del mundo serían vulnerables ante la computación cuántica. Explicándonos cómo la cuántica podría incluso llegar a dar las órdenes necesarias para vaciar nuestras cuentas bancarias o bien apoderarse de las criptomonedas. Incluso podría ir más allá y apoderarse de la inteligencia de los ejércitos. De ahí que los actuales algoritmos y protocolos de seguridad o se adaptan al cambio rápidamente y al mismo tiempo que avanza la cuántica o morirán de ahí que ya se trabaje en algoritmos post cuánticos en previsión de lo que pueda llegar del futuro un futuro cuántico que ya está aquí y ha venido para quedarse.

Desde este podio de la Real Academia queremos finalizar como nos indicó en su último discurso en Belgrado el académico y catedrático Dr. VICENTE LIERN advirtiendo que los adelantos científicos son imparables y que acabaremos abrazando irremediablemente la computación cuántica.

En consecuencia, por mucho que importantes instituciones como el Instituto de Estándares y Tecnología de los EEUU traten de evitar problemas ante ese choque anunciado y adelantándose a estos, ya se investiga con algoritmos,

para ser resistentes a la computación cuántica. Para que esta computación cuántica inexorablemente luego quede obsoleta como quedarán los bits con lo que respecta a los cubits y luego otros algoritmos y adelantos científicos las desplacen y ocupen sus lugares y esa hegemonía mundial sea cuestionada por una carrera en la que la ciencia y los académicos son y serán el futuro.

He dicho.

Dr. José Daniel Barquero Cabrero

CYBERSECURITY: ECONOMIC AND NON- ECONOMIC ASPECTS

Dr. Janusz Kacprzyk

Academico Correspondiente por Polonia de la Real Academia de Ciencias Economicas y Financieras

The purpose of this short note is to briefly presents some thoughts and remarks on one of the greatest and most dangerous threats in our civilization which is related to, maybe even caused by, an omnipresent use of new communication means related to the broadly perceived „Internet".

We will briefly present various consequence of this technological and social development, in fact even a „revolution", which can be described as follows: first, instead of the well known statement „for the humans the only fully natural means of articulation and communication is natural language", maybe the following statement is valid „for the („modern", younger?) humans the only fully natural means of articulation and communication are all kinds of „new speak" exemplified by the Internet shorthand, cyberslang, netspeak, digispeak, chatspeak, etc."

Moreover, this all is amplified by the total „stay connected" attitude and way of life, practically all technology and services fully relying on the Internet, computer networks, etc. which makes it very easy to access everybody via the Internet, steal his/her data and identity, compromise his/her privacy, etc. Needless to say that these activities can make much harm to the people, companies and institutions involved, both financial harms and those related to other aspects that can be crucial.

Unfortunately, these threats are not always taken seriously by the human beings who are the stakeholders in all intercations with and processes within such modern settings that are vulnerable to threats. Basically, the problems lies in the human psychology because the humans tend to think that since in

the present time the technology has reached a very high level of development and sophistication, then it will also manage all kinds of thereats related to that new totally stay connected settings. This is, however, not true. As very often, maybe always, the weak point is the human elements, both the wrongdoes and victims.

For the purpose of this short note cybersecurity is meant in a broad sense as being related to every aspect of safeguarding and protecting individuals and social groups, notably organizations and institutions against all kinds of cyberthreats, notably cyberattacks, which involve threats to assets, identity, personal, corporate and national security, tp just mention a few.

The broadly perceived cyberthreats (e.g. cyberattacks) rapidly grow in numbers and complexity and pose a higher and higher threat to companies, organizations, countries, and societies, not to speak about the individuals.

Therefore there is an urgent need first for a deep understanding, followed by research and investigations into all aspects of cyberthreats. This involves many issues, notably: the conceptualization and development of passive and active approaches to dealing with cyberthreats, starting form simple attempts to safeguard against them, to a proactive mitigation of associated risks.

A threat should be cosnidered from many points of view starting from the level of individuals and social groups, notably organizations or institutions, then proceeding to various area specific levels exemplified by: economic, business, military, political, etc.

In this short talk we will focus on the human being, both in the sense of an individual and a social group as the focal points of the analysis since these are the subjects to be attacked, and also subject who can counteract and safeguard against attacks and possibly even mitigate the related risks. Our emphasis will be a human indicidual if not otherwise stated. In this context we will discuss

some human specific qualities, behavior, attitudes, judgmentsm etc. that are crucial and have to be properly accounted for.

Such a perspective is a reflection of a huge research area with more and more approaches, publicatons, and also practical applications which has become popular in recent years all over the world.

Due to a lack of space, we will mention here just two important aspects:

- The use of elements of social engineering,
- The usefulness of some results of cyberpsychology.

The first question is what social engineering (of course, related to IT in our context) is. There are many views exemplified by the definitions proposed by ENISA (EU Agency for Cyber Security) that says that, first of all, the wide use of IT/ICT in all areas of human activities has implied the proliferation of „trickeries" aimed at using psychological manipulation to get further access to IT/ITC systems, for instance, via.impersonating an important client through a phone call to get into a malicious website. Moreover, by using IT/ICT technologies for psychological manipulation techniques, for instance, for obtaining banking credentials via a phishing attack to then steal the target's money.

Now, most cyberattacks include some form of social engineering. Many cybersecurity incidents are implied by targets (humans involved, wrongdoers and victims) performing specific behavioral actions, such as opening a link within a phishing email.

Cyberadversaries, the wrongdoers, employ knowledge on psychological processes related to motivation, group dynamics or social identity. Intentional and unintentional threats are associated with many psychological factors like cognitive load, mental wellbeing, trust, interpersonal relations, to just name a few. The problem is that the human nature is very complicated and, in spite

of many relevant dvelopments in the fields of psychology, cognitive sciences, sociology, etc. there still remain many open issues and unnaswered questions./

To be more specific, one can mention the following examples of social engineering based cyberattacks, mainly from in-person phone conversation to emails:

- specifically structured emails to deceive the recipient into providing information, opening an attachment, and/or clicking links,

- agents pretending to be employees or vendors trying to gain access to secured locations or information, e.g. by unexpected phone calls, often via spoofed numbers that cannot be reached directly, etc. etc.

Basically, the main problem is here trust which is the crucial element in all kinds of relationships, and hence is also widely employed by humans who want to use social engineering tools and techniques.

Some 98% of hackers use social engineering to manipulate their target individuals by using email, phone, or personal contacts to acquire confidential information. They observe specific personal features, mentality, reoccurring routine actions or relationships, all in various contexts, and try to mimick them to develop the appearance of an individual one can trust, for instance, a police officer or bank employee.

In this context one should also mention social-cybersecurity, an emerging scientific area dealing with how to characterize, understand, and forecast changes in human behavior, mentality, and social, cultural and political outcomes, and to develop the cyberinfrastructure needed for the individuals, groups and society in the new cybermediated environment, that is, characterized by changes and frequent cyberthreats. This involves an analysis of sources and intensity of attacks, threatened stakeholders, impact of attacks, mitigation of risks, etc.

Recently, one can observe a general trend in science and technology that is characterized by the exustence of the so-called big data, that is, the data that cannot be effectively and efficiently represented and processed by conventionals tools and techniques, and which constitute a basis of data driven approaches in virtually all fields of science and technology. The new field of social cybersecurity also shows a strong tendency of using modern tools and techniques exemplified by network analysis, social media analytics, data mining, machine learning, and artificial intelligence (AI).

Cyberpsychology – also known as Internet psychology, web psychology, or digital psychology – is a new emerging scientific discipline at the crossroads of many scientific disciplines. It deals with psychological phenomena resulting from, and governing human interaction with the digital technology, notably in the interconneted world, by using the Internet and WWW or, which is more and more common nowedays, social media. For instance, one of important, interesting and challenging problems is here how humans interact with each other in a virtual environment, virtual reality (VR) or even the metaverse that makes it possible to explore virtual 3D spaces in which the human being can collaborate, play, learn, etc.

The impacts of such new human – digital world intercation modes can be far reaching for both the individuals and the society. Needless to say that they will also have a huge impact on the broadly perceived cybersecurity. Issue related to the impact of disruptive technologies like artificial intelligence (AI). Some people also point out the importance of some new, more general directions exemplified by transhumanism that can be viewed as that the human beings could use technology to modify and enhance human cognitive, mental or physical abilities which are not „naturally" available due to biological constraints.

In this context, cyberpsychology investigates how the human cognition, mind and behavior are affected by new online technologies like the virtual reality (VR) or metaverse, smartphones, social media, etc. which are com-

monly used. Among many aspects, one can also mention here issues related to online identity and relations, personality types, Internet addiction, to just mention a few.

To conclude this short note, its main purpose has been to briefly provide some arguments that the problem of cybersecurity will gain more and more relevance in the future because of a growing „stay connected" attitide and way of life. For the world to function properly, both at the level of individuals, social groups, institutions and organizations, this problem should definitely be solved. A comprehensive approach is needed accounting for economic, sicial sychological, technological and engineering aspects,

The role of the human being is crucial as he/she is a decisive factor and element in any non-trivial process or system since, as it is said, „it is all about humans". This human centricity of cybersecurity makes the problem more difficult, both at the level of analyses and all kinds of mitigations of reespected problems, because of the complexity of the human being with respect to his/her judgments, reasoning, evaluations and assessments.

The human sspecific cognitive biases, exmplified by the (in)famous status quo bias the essence of which is that the humans as a rule do not like changes and prefer to stay as is or the bandwagon effect in that the humans tend to do what most do, etc. make the problem ven more difficult.

Results from various felds of science should be employed, mainly from economics (humanistic economics?), social sciences, lsychology, cognitve sciences,applied mathematics, systems science, etc. etc. to obtain meaning full results.

EL HUMANISMO COMO MARCO DE LA ACTIVIDAD EMPRESARIAL

Dr. Mario Aguer Hortal
Académico de Número de la Real Academia de Ciencias Económicas y Financieras

RESUMEN

En esta ponencia se hace un estudio de las aportaciones del Humanismo a la empresa, haciendo una breve presentación de los orígenes del humanismo aplicado a la economía sobre todo en lo que hace referencia a la Escuela Humanista de Barcelona. Se hace hincapié en los actuales paradigmas a los que se enfrenta la actividad empresarial como son el cambio climático, los conflictos regionales y la inteligencia artificial entre otros.

1. Introducción

El concepto de humanismo aplicado a la actividad empresarial no es nuevo y podrían rastrearse algunos rasgos parecidos en la temprana Liga Hanseática, la famosa y exitosa federación comercial de comunidades de comerciantes alemanes en el mar Báltico y los Países Bajos. La visión de la liga no era solo comercial, también lo era colonizadora y exportadora de una forma de "hacer" que aún perdura en nuestros días, así por ejemplo Hamburgo y Bremen, los centros impulsores, siguen teniendo el rango de ciudad estado. Sin embargo el concepto aceptado actualmente es mucho más moderno. Podemos situar sus orígenes en distintos focos desde los que se expandió el concepto. Uno de ellos es el instituto de la Universidad de Navarra, Empresa y Humanismo que, con un enfoque multidisciplinar y humanista, intenta aportar soluciones a los problemas que surgen en la sociedad en el ámbito de la actividad económica colocando la persona en el foco de su atención. En esta línea destacaron empresarios como José María Zalbidea y Tomás Calleja de Iberdrola, Felipe Gómez de IBM y Manuel Herrán de la Compañía Sevillana de Electricidad.

Hay que matizar que el grupo de Navarra no estaba centrado únicamente en la actividad empresarial sino también en otros ámbitos de naturaleza asociativa y cultural. Otro foco es la Escuela Humanista de Barcelona, en la que, de forma más exclusiva, se asientan las bases del humanismo empresarial. Esto ha sido posible, principalmente, al entender que la persona es el sujeto de la actividad económica en su integridad, es decir, con su carga de razón y su carga de imaginación, de objetividad y de subjetividad, tanto en la planificación como en sus decisiones.

Vale la pena reproducir un fragmento del discurso del profesor Jaime Gil Aluja, pronunciado el 7 de febrero de 2022 invitando a instituciones e investigadores a sumarse a la Escuela de Economía Humanista de Barcelona de la Real Academia de Ciencias Económicas y Financieras para renovar y aportar una nueva herramienta al pensamiento económico, reanudando una vieja tradición iniciada en Barcelona en 1986 por los profesores Arnold Kaufmann, Lofti Zadeh, Jacques Pezé y el propio Gil Aluja.

"Ante la necesidad de renovar el pensamiento económico para desentrañar la creciente complejidad de nuestras economías y los desafíos de la digitalización, consideramos necesario reivindicar la tradición iniciada en 1986 por la Escuela de Economía Humanista de Barcelona, con las aportaciones seminales de los profesores Arnold Kaufmann, Lofti Zadeh, Jacques Pezé y quien hoy preside esta Real Corporación, Jaime Gil Aluja. Sus aportaciones permitieron renovar el paradigma del análisis de las estructuras económicas desde un enfoque humanista que no había sido alcanzado por escuelas anteriores y que creemos más necesario que nunca. Es por lo que hacemos llamamiento a cuantos han participado y participan de esta línea de investigación y análisis en Barcelona durante estas décadas y que siguen aportando sus conocimientos y trabajo a la ciencia económica desde universidades y centros de investigación en todo el mundo para que se adhieran a esta iniciativa con el fin de renovar, difundir y aplicar nuestros conocimientos en la búsqueda de nuestra prosperidad compartida".

2. El Humanismo Empresarial

Cuando nos preguntamos qué es el humanismo empresarial, la primera respuesta es dar algunos ejemplos de lo que nosotros entendemos qué debería ser y, en general, solemos recurrir a conceptos morales más o menos relacionados con creencias éticas, morales o religiosas, o bien nos adentramos en aspectos matemáticos cuando postulamos la aplicación de la lógica difusa a los problemas que plantea la gestión empresarial. El humanismo empresarial según el enfoque de la Escuela de Economía Humanista de Barcelona, no está ligado a ninguna práctica religiosa, aunque tampoco tiene porqué ser contraria a sus principios. Se trata más bien de unos postulados basados en el sentido común, el cumplimiento de la ley y lo que podríamos llamar expansión de objetivos sin olvidar el eje vertebrador de la actividad empresarial que es la obtención de beneficios. Se trataría de utilizar un metalenguaje para normalizar el lenguaje que utilizaremos, o si queremos verlo desde otro ámbito, una metanorma que dé consistencia a las normas del humanismo. El introductor del concepto es Robert Axelrod profesor de Ciencias Políticas de la Universidad de Michigan autor de la obra de referencia "Evolution of Cooperation" de 1984. La actividad empresarial requiere un marco jurídico que regule los derechos y deberes no solo entre el propietario de la empresa y los trabajadores sino entre vendedores y compradores o entre prestadores de un servicio y los clientes que lo utilizan. Si este marco es débil la actividad empresarial se fragiliza y hasta puede desaparecer. Sobre la aplicación de la lógica difusa a la gestión económica poco hay que decir sobre una técnica muy fructífera que se ajusta como un guante a la actividad humana que huye del eterno dualismo entre blanco y negro. La realidad está inundada de grises y en este fértil jardín se desenvuelve la lógica difusa, también llamada de Fuzzy.

3. Elogio del sentido común

Hay conceptos que por obvios no suelen tener mucho predicamento; uno de ellos es el sentido común. El sentido común, "sensus communis", es lo contrario de la intuición. Está basado en la lógica, la experiencia, el co-

nocimiento. La intuición no es contraria a la actividad empresarial y puede jugar un importante papel en la toma de decisiones para adivinar el comportamiento del mercado y sobre todo de lo que demanda. Pero la intuición si no está sujeta a un férreo análisis posterior queda reducida a pura lotería especulativa. La intuición representa una luz que se vislumbra sobre un fondo de oscuridad, el sentido común representa el trabajo constante, medido, tenaz, el día a día de la actividad empresarial. En realidad la práctica del sentido común está muy relacionada con una forma de ser reflexiva y poco impetuosa; de todas formas si queremos saturarnos de sentido común es útil leer los "Pensamientos" de Marco Aurelio o los "Ensayos" de Michel Montaigne, libro que algunos elevan a la categoría de obra maestra. Dentro de las múltiples acepciones que tiene el concepto prevalece la de "hacer lo razonable". Este hipotético valor no está exento de crítica. Hacer lo razonable parece indicar "ir por el camino adecuado", pero esta afirmación carece de valor científico en tanto que no definimos científicamente las distintas posibilidades ni las soluciones óptimas en cada caso. También puede influir la orientación de la sociedad, la moda, la época, la edad y muchos otros factores que algunos tildarían de prejuicios. Así, por ejemplo, el sentido común de un agresivo empresario americano no puede ser el mismo que el de un empresario japonés mucho más conservador y tradicionalista. El sentido común tiene detractores pero estoy firmemente convencido de su utilidad siempre que entendamos que se trata siempre de una forma de transitar, de enfocar un problema, dicho de otra forma y para terminar, el sentido común debe ser un método más que una solución.

4. La expansión de objetivos

4.1 Introducción

Cualquier empresario estará de acuerdo en que el principal objetivo de su actividad es la obtención de beneficios pues de otra forma no tendría sentido la inversión realizada. Pero, ¿debe ser el único objetivo?

Uno de los objetivos empresariales, quizá el más importante, es obtener la mayor cantidad de resultados que después se traducirán en beneficios. En lo que sigue daremos por supuesto que hay que hacerlo teniendo presente, y acatando, la normativa legal a la que esté sujeta la empresa. De otro modo estaríamos hablando de actividades ilícitas. Sin embargo hay una diferencia entre respetar la normativa o actuar de forma humanista. Por ejemplo una empresa que se dedica a la fabricación de componentes electrónicos, puede abrir una planta en un país en vías de desarrollo en la que respetará toda la normativa legal, pero los trabajadores tendrán un sueldo de miseria y unos derechos laborales inexistentes. Es evidente que aquella planta brindará unos beneficios muy superiores a la que tendría de estar situada en un país más avanzado económica y socialmente.

El 25 de diciembre de 1925 se fundó la empresa I. G. Farbenfabriken como una fusión de BASF, BAYER y HOESCHST; a partir de 1934 empieza a fabricar el gas Zyklon B que se utiliza en Stutthof, Mausthausen, Sachsenhausen y Ravensbrueck para exterminar judíos, gitanos, rumanos, alemanes disidentes y disminuidos a un ritmo que en Mausthausen llegó a los 12.000 diarios. Está claro que los objetivos de una empresa pueden ser diferentes y variados, pero también siniestros.

No siempre puede controlarse el destino un producto, sobre todo si se trata de componentes electrónicos, energía, acero, petróleo o armamento. No podemos ser o aparentar ingenuidad. Sabemos que las armas son necesarias pero no es lo mismo suministrarlas a un país que respeta los derechos humanos que a otro que no lo hace.

Hoy día el mundo se enfrenta a unos desafíos que debemos tener muy presentes: la creciente contaminación, el cambio climático, la falta creciente de agua y de recursos en general y la proliferación de conflictos armados que pueden llegar a ser nucleares a nivel regional. Todos estos desafíos son difíciles de solucionar (o de mitigar) pero todos ellos pueden tener efectos catastróficos para la humanidad. La idea central de mi exposición es que cuando hablamos

de objetivos valdría la pena pensar no solo en los económicos. ¿Contamina nuestra empresa? ¿Nuestros productos caerán en malas manos? ¿Abrimos una sucursal en un país que no respeta los derechos humanos? ¿Emitimos una cantidad desproporcionada de CO_2? ¿Aumentamos beneficios contratando ilegalmente? Son preguntas para la reflexión.

4.2 El aumento imparable de la contaminación

En el Pacífico hay una isla de basura que triplica el tamaño de Francia y es el mayor vertedero oceánico del mundo de plástico flotante que mata, cada año, a miles de animales marinos entre California y Hawái. Algunos la llaman el séptimo continente. La contaminación no solo implica plástico, también residuos (sin olvidar los nucleares), lluvia ácida, gases nocivos y contaminantes, productos tóxicos y muchos otros. ¿La única solución es trasladar la fábrica a un país que haga la vista gorda? Evidentemente no se trata solo de la contaminación de los plásticos, también del aire, del agua dulce de ríos y lagos, así como la marítima. Sin olvidar la ingente cantidad de residuos urbanos e industriales que generamos y sobre todo los nucleares, verdadera pesadilla del futuro. De momento la única solución eficaz de la que disponemos es la reutilización; actualmente se está trabajando en el diseño, por manipulación genética, de bacterias que se alimenten de plástico, pero aún estamos lejos.

4.3 El cambio climático

El efecto invernadero (el CO_2 que producimos deja pasar la radiación de onda corta pero no deja salir la de onda larga) producirá en los próximos años un aumento medio de la temperatura que puede ser entre los 1,5 y los 3º C, de efectos devastadores: 1) aumento del nivel del mar, 2) avance imparable de la desertización, 3) fenómenos atmosféricos más virulentos y 4) sobre todo un aumento incontrolable de la emigración de los habitantes de las zonas cálidas hacia las templadas y frías. Los expertos temen mucho más este último efecto que los otros. Si tenemos dudas al respecto consultemos con el google la población de Egipto, de Nigeria, del Congo, de Etiopía por citar solo estados

africanos. ¿Qué ocurrirá con esta población cuando no puedan vivir en su país?

Para luchar contra el cambio climático es necesario: 1) reducir las emisiones de CO_2, 2) promover y utilizar el coche eléctrico, 3) no hacer barbaridades con nuestros bosques, 4) reducir la dependencia energética del petróleo, 5) promover las energías renovables, todas ampliamente conocidas y poco practicadas. Ahora asistimos a un auge espectacular del coche eléctrico, que tiene unas virtudes propias, como por ejemplo que al no estar sujeto al factor de Carnot, puede tener rendimientos muy superiores al de combustión y que, además, no contamina "in situ". Sin embargo el coche eléctrico consume electricidad que se produce en una central eléctrica, si ésta es térmica no resolvemos el problema de fondo porque nuestro vehículo sigue consumiendo combustible fósil por intermedio de la central. Solo en el caso de que la electricidad consumida sea de procedencia renovable cerraremos el círculo de la bondad de la medida.

Los expertos señalan que a medio plazo se vislumbra la posibilidad de utilizar el hidrógeno, no como recurso, que no lo es, sino como vector energético. El hidrógeno es como si tuviésemos energía encapsulada con un poder calorífico cuatro veces superior al del petróleo. El hidrógeno ha de fabricarse y para ello se consume energía en el proceso de fabricación. Esta energía siempre será superior a la que libere posteriormente el hidrógeno. Sin embargo el hidrógeno puede obtenerse por electrólisis del agua utilizando electricidad fotovoltaica; en este caso la energía liberada por el hidrógeno sería indirectamente renovable y, además, limpia, porque la combustión del hidrógeno no produce CO_2. Detrás de este proceso se esconde otra maravilla tecnológica. Es posible producir directamente electricidad a partir del hidrógeno; el convertidor es la *pila de combustible* o "fuel cell". La pila de combustible tampoco está sujeta al factor de Carnot y por lo tanto su rendimiento puede ser muy elevado. Es posible ir mucho más allá; de hecho, Rifkin, llamado el gurú del hidrógeno, postula una teoría llamada "revolución del hidrógeno" donde pronostica la creación de una red energética mundial de empresas y particulares que no

serían dependientes de los centros monopolizadores. Algo así como la red de internet aplicada a la producción de energía eléctrica. Personalmente considero un tanto visionario a Rifkin, que por otra parte ha sido asesor de distintos gobiernos americanos y europeos, pero ¿qué sería el mundo sin aportaciones revolucionarias que sacudan los cimientos del inmovilismo?

4.4 La falta creciente de agua potable y de recursos en general

Las causas son: 1) la superpoblación y 2) el cambio climático que empieza a ser evidente en muchos sitios. Fenómenos como la desertización creciente, el aumento de la temperatura media, los cultivos intensivos, la tala de bosques provocan esta alarmante carestía que está produciendo estragos en amplias zonas sobre todo africanas.

4.5 La proliferación de conflictos armados

Digo conflictos nucleares a nivel regional porque si son a nivel global la historia de lo que suceda la escribirán otros. El derrumbe de la Unión Soviética ha propiciado una inestabilidad no solo entre naciones sino también entre bloques que pugnan por la supremacía. La China pisa los talones a Estados Unidos que no quiere perder su supremacía, la Unión Europea no acaba de encontrar su lugar y Rusia sueña con grandezas de otra época. El eterno conflicto entre Israel y los Países Árabes emponzoña el Oriente Medio y los países africanos ahora escuchan los cantos de sirena de unos que acabarán haciendo lo mismo que hicieron los otros.

4.6 La inmigración

Podríamos considerar la inmigración como una consecuencia del cambio climático, pero es algo más. Se trata de un fenómeno global que puede adquirir dimensiones dramáticas de forma puntual. Tiene aspectos positivos. En los países avanzados se produce generalmente un envejecimiento de la población que conduce a la utilización foránea de mano de obra. También puede

haber causas coyunturales como ocurrió en Alemania tras la segunda guerra mundial. Pero es evidente que una emigración masiva y descontrolada desestabiliza el país receptor, hace disminuir la tasa de prestaciones sociales y crea guetos y bolsas de población mal adaptadas. Se necesitan generaciones para corregir estos problemas y sus efectos son muy inquietantes cuando se añaden fobias culturales o religiosas. La emigración debe ser controlada, sin olvidar que abandonar en alta mar a una embarcación precaria de subsaharianos es un asesinato puro y duro.

4.7 Inteligencia artificial

La inteligencia artificial, IA, está de moda y creo que no tiene marcha atrás, para bien o para mal. Grandes compañías están embarcadas en una guerra de supremacía para ver quién se lleva el gato al agua. Grandes éxitos jalonan su singladura, pero también es cierto que algunos nubarrones apuntan problemas en el horizonte. ¿Tiene límite la IA? ¿Superará la humana? ¿Podremos controlarla? Hoy día es frecuente ver a gente que se dirige a su ordenador o móvil como si fuera una persona, ordenándole que llame a fulano o que tal o cual cosa. ¿Se irá perdiendo el uso de la escritura? ¿Autorizaremos a nuestro móvil a tomar decisiones que nos afecten? Ignoro la respuesta a estas preguntas pero el simple hecho de formularlas es un indicio de la importancia del tema.

4.8 Protección al consumidor

Proteger y garantizar los derechos de los clientes o, si se trata de una empresa de servicios, de los consumidores, debe ser un objetivo ineludible de la actividad empresarial. Un cliente o consumidor satisfecho, es un reclamo que a medio y largo plazo incrementará la demanda del bien producido. Y no nos referimos únicamente a los derechos clásicos, como podrían ser el respeto de los plazos de devolución o de reparación de un producto o de la atención de proximidad sino también a los derivados de la seguridad respecto a las modernas técnicas informáticas, que hoy han hecho posible la expansión de tantas

y tantas empresas. La ciberseguridad es hoy una necesidad de primer orden debido a la forma como hoy se desenvuelve la actividad comercial. El uso de datos bancarios y personales de los clientes obliga a ser muy cuidadoso con las operaciones en los que éstos se ven expuestos procurando líneas de defensa ante agresiones que podrían perjudicarlos. De todos es conocida la proliferación de ataques piratas a empresas y grandes centros con el objetivo de cobrar un rescate para evitar la divulgación fraudulentas de datos personales de clientes. La ciberseguridad debe ser norma y objetivo y cada vez serlo más.

5. Conclusión

No pensemos que un cambio de mentalidad pueda introducirse con rapidez sobre todo en un mundo, el empresarial, en el que las inercias marcan un ritmo propio poco propenso a los cambios. Sin embargo nunca está de más quitar el polvo, abrir las ventanas y que entre un poco de aire fresco. Los retos futuros, que a medio plazo debe enfrentar la humanidad, serán una medida de la capacidad de la gente para entender que la política de bloques, el ultranacionalismo y la cortedad de miras de algunos políticos actuales nos conduce irremediablemente a una situación de permanente conflicto que debemos superar con la cooperación, la justicia y el progreso científico.

La lucha contra el cambio climático puede tener efectos colaterales positivos. Hace tiempo que predicamos a favor de las energías renovables, del coche eléctrico, del hidrógeno como vector energético y quizá, con un poco de suerte, esta crisis puede acelerar el cambio de paradigma.

Los empresarios no son la solución del problema, pero sin ellos no hay problema ni solución; seguiríamos siendo la tribu paleolítica de cazadores recolectores. Pensemos que en un cierto momento mágico de la historia humana, alguien se dio cuenta que la tribu disponía de un cierto excedente, que podía ser carne curada, herramientas de sílex o conchas marinas para hacer amuletos y se hizo la pregunta de ¿porqué no intercambiamos, con la tribu vecina, este producto por otro que necesitemos más? Éste fue el primer em-

presario y el mundo cambió. Y el mundo volverá a cambiar cuando el empresario comprenda que no se trata de ganar sólo dinero sino de hacerlo con una finalidad no egoísta, es decir, que tenga en cuenta no sólo la felicidad propia sino también la general.

Actualmente estamos inmersos en la llamada revolución de la información; las empresas, tanto las públicas como las privadas, acumulan más y más información sobre más gente. Es un deber proteger esta información. No olvidemos que la ciberseguridad debe ser uno de los modernos paradigmas para cualquier gestor o empresario.

BIBLIOGRAFÍA

AGUER M., MIRANDA A. L. (2007) *El hidrógen. Fundamento de un futuro equilibrado*. Madrid: Ed. Díaz de Santos.

AXELROD R. (2007) *Evolution of Cooperation*. London: Ed. Basic Books.

BRAUDEL F. (1995) *A History of Civilizations*. New York: Ed. Penguin Publishing Group.

GIL ALUJA J. (1990) *Matemáticas del azar y de la incertidumbre*. Madrid: Editorial Universitaria Ramón Areces.

GRASSI E. (1993): *La filosofía del humanismo. Preeminencia de la palabra*. Barcelona: Ed. Anthropos.

KAUFMANN A., GIL ALUJA J. (1986) *Introducción a la teoría de subconjuntos borrosos a la gestión de las empresas*. Santiago de Compostela: Ed. Milladoiro.

KAUFMANN A. GIL ALUJA J. (1987) *Técnicas operativas de gestión para el tratamiento de la incertidumbre*. Barcelona: Ed. Hispano Europea.

LLORENS M., MIRANDA A. L. (2009) *Ingeniería térmica*. Barcelona: Ed. Marcombo

MARCO AURELIO (2020) *Pensamientos*. Madrid: Ed. EDAF.

MONTAIGNE M. (2021) *Ensayos*. Madrid: Ed. El Acantilado.

RIFKIN J. (2002) La economía del hidrógeno. La creación de la red energética mundial y la redistribución del poder en la tierra. Barcelona: Editorial Paidós.

SANTANA L. (2013) "Una aplicación de la lógica difusa a la evaluación del balance de riesgos de la inflación y del crecimiento macroeconómico" en *Ciencia y Sociedad*, 38 (3): 497-514

CLAUSURA DEL
II ACTO INTERNACIONAL DE PRIMAVERA
DE BARCELONA

EL TRATAMIENTO DE LA SUBJETIVIDAD, UN NUEVO HORIZONTE PARA LA CIBERSEGURIDAD

Dr. Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas y Financieras

Una vez más, la llamada a la colaboración de los investigadores con objeto de unir voluntades para la investigación económica avanzada ha sido bien recibida.

Nos hemos reunido en nuestra sede de la Real Academia de Ciencias Económicas y Financieras de España para escudriñar, dentro de las realidades sociales de hoy y fijando la atención en la neblina del futuro, como serán nuestras vidas consideradas de manera individual y colectiva en el marco de un mañana del que solo atisbamos sus componentes de complejidad y de incertidumbre.

Después de la densas sesiones, en las que han surgido interrogantes y propuestas, decisiones y programas, ya podemos afirmar, sin que ello nos cause rubor, que estamos caminando en la buena dirección y que la ciberseguridad que concebimos, no solo no va a entorpecer los legítimos objetivos económicos dentro del marco jurídico en el que nos hallamos inscritos, si no tampoco lo van a hacer los objetivos morales, en concordancia incluso con los códigos no inscritos de una ética que la sostenibilidad de nuestro planeta los hace cada vez más imprescindibles.

De una manera u otra, nos ha parecido colegir de las ponencias presentadas, una confluencia hacia algo que es consustancial con los trabajos de nuestra Real Corporación: la idea de **Escuela de Economía Humanista de Barcelona**.

Nos referimos a la incorporación en las **nociones básicas** a establecer para conformar el desarrollo de los procesos destinados a la creación y diseño de la ciberseguridad, tanto en lo que se refiere a los propios procesos como a la utilización de los mismos: los criterios definidores **pueden** y en la mayor parte de los casos **deben** tener no solo carácter objetivo sino también subjetivo.

Esta conclusión, siempre provisional, es el resultado incuestionable del doble objetivo último buscado: económico y moral.

Hasta aquí, no parece que existan disidencias apreciables. Estas aparecen cuando se avanza un paso más y se abordan las tareas de optimización numérica o no numérica de los procesos de diseño de la ciberseguridad.

Desde la más elevada formalización, nos hemos dado cuenta que, al problema multicriterio se ha añadido otro de naturaleza calculatoria: la compatibilización de datos objetivos y subjetivos, sin perder información. Lofti Zadeh nos señaló el camino para hacerlo[1] y lo hemos hecho en multitud de ocasiones.

Y lo hemos hecho tanto en temas de elevada abstracción como en los más cercanos a la aplicación de todos los procesos calculatorios: los algoritmos.

En el futuro no sabemos si seremos capaces de hacerlo solos, pero de lo que sí estamos convencidos es que podremos lograrlo con creces juntos, trabajando en estrecha colaboración científica.

Desde este púlpito, que generosamente nos han prestado durante estos minutos, exhortamos a todos cuantos formamos parte del **humanismo económico**, para que continuemos por esta senda a fin de situar a la Real Corporación que nos acoge, junto a las más prestigiosas instituciones de investigación económica avanzada.

1 Zadeh, L. A.: “Fuzzy Serts: Information and control”, 8 (3), 1965

Que en el retorno a cada uno de nuestros hogares, nos acompañe la ilusión y la voluntad de servicio. Hasta siempre.

El acto ha terminado. Se levanta la sesión.

Gracias, muchas gracias.

BIBLIOGRAFÍA

Gil Aluja, J.: "Elements for a Theory of Decision in Uncertainty". Kluwer Academic Publishers. Dordrech, Boston, Londres, 1999. (ISBN: 0-7923-5987-9)

Kaufmann, A.: "Les logiques humaines et arficielles" Ed. Hermes, París, 1988. (ISBN: 2-86601-137-6).

Kaufmann A. y Gil Aluja J.: "Técnicas operativas de gestión para el tratamiento de la incertidumbre". Ed. Hispano Europea. Barcelona, 1987. (ISBN: 84-255-0775-8)

Kaufmann A. y Gil Aluja, J.: "Introducción de la teoría de los subconjuntos borrosos a la gestión de las empresas" Ed. Milladoiro, Santiago de Compostela, 1986. (ISBN: 84.398-7630-0)

Kaufmann A. y Gil Aluja, J.: "Grafos neuronales para la economía y gestión de empresas". Ed. Pirámide. Madrid 1995. (ISBN: 84-318-0917-3)

Kaufmann, A., Gil Aluja, J. y Gil Lafuente A.M.:"La creatividad en la gestión de las empresas". Ed. Pirámide. Madrid, 1994. (ISBN : 84-368-0800-2)

Pichat, E.: " Contribution a l'algorithmique non numerique dans les ensembles ordonnés" Tesis doctoral de Ciencias. Universidad de Grenoble, 1970.

Prigogine, Ilya: “La fin des certitudes”. Versión española con el título: « El fin de las certidumbres ». Ed. Taurus, Buenos Aires, 1997. (ISBN: 84-306-0025-6)

Zadeh , Lotfi A.: “Fuzzy Sets”. Information and Control 8 (3) 1965.

Real Academia
de Ciencias Económicas y Financieras

PUBLICACIONES DE LA REAL ACADEMIA DE CIENCIAS ECONÓMICAS Y FINANCIERAS

*Las publicaciones señaladas con el simbolo
están disponibles en formato PDF en nuestra página web:
https://racef.es/es/publicaciones

***Las publicaciones señaladas con el símbolo o
están disponibles en nuestros respectivos canales de Youtube y Vimeo

PUBLICACIONES DEL OBSERVATORIO DE INVESTIGACIÓN ECONÓMICA Y FINANCIERA

M-24/11 *Nuevos mercados para la recuperación económica: Azerbaiyán.*

M-30/12 *Explorando nuevos mercados: Ucrania, 2012. (Incluye DVD con textos en ucraniano), 2012.*

M-38/15 *Desarrollo de estrategias para la cooperación económica sostenible entre España y México, 2015.*

M-41/16 *Cuba a la luz de la Nueva Ley de Inversiones Extranjeras: Retos y oportunidades para la economía catalana, (Estudio elaborado por el Observatorio de Investigación Económico- Financiera), 2016.*

MO-47/16 *Colombia: la oportunidad de la paz. Estudio sectorial para la inversión de empresas españolas en el proceso de reconciliación nacional (Estudio del Observatorio de Investigación Económico-Financiera de la RACEF).*

MO-50/17 *La gestión y toma de decisiones en el sistema empresarial cubano. Gil-Lafuente, Ana Maria; García Rondón, Irene; Souto Anido, Lourdes; Blanco Campins, Blanca Emilia; Ortiz, Torre Maritza; Zamora Molina, Thais.*

MO-52/18 *Efectos de la irrupción y desarrollo de la economía colaborativa en la sociedad española. Gil-Lafuente, Ana Maria; Amiguet Molina, Lluís; Boria Reverter, Sefa; Luis Bassa, Carolina; Torres Martínez, Agustín; Vizuete Luciano, Emilio.*

MO-53/19 *Índice de equidad de género de las comunidades autónomas de España: Un análisis multidimensional. Gil-Lafuente, Ana Maria; Torres Martínez, Agustín; Boria Reverter, Sefa; Amiguet Molina, Lluís.*

MO-54/19 *Sistemas de innovación en Latinoamérica: Una mirada compartida desde México, Colombia y Chile. Gil-Lafuente, Ana M.; Alfaro-García, Víctor G.; Alfaro-Calderón, Gerardo G.; Zaragoza-Ibarra, Artemisa; Goméz-Monge, Rodrigo; Solís-Navarrete, José A.; Ramírez-Triana, Carlos A.; Pineda-Escobar, María A.; Rincón-Ariza, Gabri- ela; Cano-Niño, Mauricio A.; Mora-Pardo, Sergio A.; Nicolás, Carolina; Gutiérrez, Alexis; Rojas, Julio; Urrutia, Angélica; Valenzuela, Leslier; Merigó, José M.*

MO-56/19 *Kazakhstan: An Alliance or civilizations for a global challenge. Ministry of National Economy of the Republic of Kazakhstan – Institute of Economic Research; Royal Academy of Economic and Financial Sciences of Spain.*

MO-60/19 *Medición de las capacidades de innovación en tres sectores primarios en Colombia. Efectos olvidados de las capacidades de innovación de la quínoa, la guayaba y apícola en Boyacá y Santander. Blanco-Mesa, Fabio; León-Castro, Ernesto; Velázquez-Cázares, Marlenne; Cifuentes-Valenzuela, Jorge; Sánchez-Ovalle, Vivian Ginneth.*

MO-61/19 *El proceso demográfico en España: análisis, evolución y sostenibilidad. Gil-Lafuente, Ana M.; Torres-Martínez, Agustín; Guzmán-Pedraza, Tulia Carolina; Boria-Reverter, Sefa.*

MO-64/20 *Capacidades de Innovación Ligera en Iberoamérica: Impliaciones, desafíos y sinergias sectoriales hacia el desarrollo económico multilateral. Alfaro-García, VG.; Alfaro-Calderón, GG.; García-Orozco, D.; Zaragoza-Ibarra, A.; Boria-Reverter, S.; Gómez-Monge, R.*

MO-65/20 *El adulto mayor en España: Los desafíos de la sociedad ante el envejecimiento. Gil-Lafuente, Ana M.; Torres-Martínez, Agustín; Guzmán-Pedraza, Tulia Carolina; Boria-Reverter, Sefa.*

MO-68/21 *Public policy to handle aging: the seniors' residences challenge / Políticas para la gestión pública del envejecimiento: el desafío de las residencias para personas mayores. Kydland, F.; Kydland, T.; Valero Hermosilla, J. y Gil-Lafuente, Ana M.*

MO-70/21 *Ecología y tecnología para una nueva economía poscovid-19. Ana María Gil-Lafuente, Agustín Torres-Martínez, Tulia Carolina Guzmán-Pedraza, Sefa Boria-Reverter.*

MO-80/23 *Cómo envejecemos los españoles: Enfermedades prevalentes y morbilidad en nuestra senectud. Ana María Gil-Lafuente, , Sefa Boria-Reverter, Lourdes Souto Anido, Emilio Vizuete Luciano, Jaime Gil Lafuente.*

MO-82/23 *Sostenibilidad Urbanística y Vivienda. Aline Castro-Rezende, Ana María Gil-Lafuente, Lluís Amiguet Molina, Luciano Barcellos-Paula, Sander Laudy.*

MO-83/23 *Innovación Tecnológica, modelos Computacionales y Sostenibilidad en Iberoamérica. Dirección Ana Maria Gil-Lafuente.* ***Autores: Argentina:*** *Lucila Lazzari, Luisa; Fernández, María José; Parma,Andrea; Landolfi, Bettina; Goyheix, Daniela; Douelle, Matías;* ***Brasil:*** *Valotto Patuzzo, Genilson; França Naves, Thiago; Ono Fonseca, Keiko Verônica; Teresinha Beuren, Arlete; Reitz Cardoso, Flávia Aparecida; Delisandra Feltrim, Valéria;* ***Chile:*** *Olazabal-Lugo, Maricruz; Espinoza-Audelo, Luis Fernando; Perez-Arellano, Luis A.; Huesca-Gastelum, Martin I.; Delgadillo-Aguirre, Alicia; Leon-Castro, Ernesto;* ***Colombia:*** *Blanco-Mesa, Fabio; Abril-Teatin, Jheisson;* ***Cuba:*** *Souto Anido, Lourdes; Imbernó Díaz, Ana Laura;* ***Ecuador:*** *Pilar Tamayo Herrera, Aracely; Tapia, Freddy;* ***España:*** *Gil-Lafuente, Ana Maria; Boria-Reverter, Sefa; Torres Vergara, Carlos;* ***México:*** *García-Orozco, Dalia; Merino Arteaga, Ireri Patricia; Alfaro-García, Víctor G.;* ***Perú:*** *Barcellos de Paula, Luciano;* ***Portugal:*** *Castro Rezende, Aline.* .

MO-84/24 *Crecimiento sostenible en España: Los retos del pacto mundial. Ana Maria Gil-Lafuente, Josefa Boria Reverter, Darley Biviana Pacheco Cubillos.* .

OTRAS PUBLICACIONES Y COEDICIONES DE LA REAL ACADEMIA

M-1/03 *De Computis et Scripturis (Estudios en Homenaje al Excmo. Sr. Dr. Don Mario Pifarré Riera), 2003.*

M-2/04 *Sesión Académica de la Real Academia de Ciencias Económicas y Financieras en la Académie du Royaume du Maroc (Publicación del Solemne Acto Académico en Rabat el 28 de mayo de 2004), 2004.*

M-3/05 *Una Constitución para Europa, estudios y debates (Publicación del Solemne Acto Académico del 10 de febrero de 2005, sobre el "Tratado por el que se establece una Constitución para Europa"), 2005.*

M-4/05 *Pensar Europa (Publicación del Solemne Acto Académico celebrado en Santiago de Compostela, el 27 de mayo de 2005), 2005.*

M-5/06 *El futuro de las relaciones euromediterráneas (Publicación de la Solemne Sesión Académica de la R.A.C.E.F. y la Universidad de Túnez el 18 de marzo de 2006), 2006.*

M-6/06 *Veinte años de España en la integración europea (Publicación con motivo del vigésimo aniversario de la incorporación de España en la Unión Europea), 2006.*

M-7/07 *La ciencia y la cultura en la Europa mediterránea (I Encuentro Italo-Español de la Real Academia de Ciencias Económicas y Financieras y la Accademia Nazionale dei Lincei), 2007.*

M-8/07 *La responsabilidad social de la empresa (RSE). Propuesta para una nueva economía de la empresa responsable y sostenible, 2007.*

M-9/08 *El nuevo contexto económico-financiero en la actividad cultural y científica mediterránea (Sesión Académica internacional en Santiago de Compostela), 2008.*

M-10/08 *Pluralidad y unidad en el pensamiento social, técnico y económico europeo (Sesión Académica conjunta con la Polish Academy of Sciences), 2008.*

M-11/08 *Aportación de la ciencia y la cultura mediterránea al progreso humano y social (Sesión Académica celebrada en Barcelona el 27 de noviembre de 2008), 2009.*

M-12/09 *La crisis: riesgos y oportunidades para el Espacio Atlántico (Sesión Académica en Bilbao), 2009.*

M-13/09 *El futuro del Mediterráneo (Sesión Académica conjunta entre la Montenegrin Academy of Sciences and Arts y la Real Academia de Ciencias Económicas y Financieras, celebrada en Montenegro el 18 de mayo de 2009), 2009.*

M-14/09 *Globalisation and Governance (Coloquio Internacional entre la Real Academia de Ciencias Económicas y Financieras y el Franco-Australian Centre for International Research in Management Science (FACIREM), celebrado en Barcelona los días 10-12 de noviembre de 2009), 2009.*

M-15/09 *Economics, Management and Optimization in Sports. After the Impact of the Financial Crisis (Seminario Interncional celebrado en Barcelona los días 1-3 de diciembre de 2009), 2009.*

M-16/10 *Medición y Evaluación de la Responsabilidad Social de la Empresa (RSE) en las Empresas del Ibex 35, 2010.*

M-17/10 *Desafío planetario: desarrollo sostenible y nuevas responsabilidades (Solemne Sesión Académica conjunta entre l'Académie Royale des Sciences, des Lettres et des Beaux-Arts de Bélgica y la Real Academia de Ciencias Económicas y Financieras de España, en Bruselas el día 8 de Junio de 2010), 2010.*

M-18/10 *Seminario analítico sobre la casuística actual del derecho concursal (Sesión Académica celebrada el 4 de junio de 2010), 2010.*

M-19/10 *Marketing, Finanzas y Gestión del Deporte (Sesión Académica celebrada en la Real Academia de Ciencias Económicas y Financieras en diciembre de 2009). 2010*

M-20/10 *Optimal Strategies in Sports Economics and Management (Libro publicado por la Editorial Springer y la Real Academia de Ciencias Económicas y Financieras). 2010*

M-21/10 *El encuentro de las naciones a través de la cultura y la ciencia (Solemne Sesión Académica conjunta entre la Royal Scientific Society de Jordania y la Real Academia de Ciencias Económicas y Financieras de España, en Amman el día 8 de noviembre de 2010). 2010.*

M-21B/10 *Computational Intelligence in Business and Economics (Proceedings de MS´10 International Conference celebrada en Barcelona los días 15-17 de julio de 2010). Edición de World Scientific, 2010.*

M-22/11 *Creación de valor y responsabilidad social de la empresa (RSE) en las empresas del IBEX 35. 2011.*

M-23/11 *Incidencia de las relaciones económicas en la recuperación económica del área mediterránea (VI Acto Internacional celebrado en Barcelona el 24 de febrero de 2011), (Incluye DVD con resúmenes y entrevistas de los ponentes) 2011.*

M-25/11 *El papel del mundo académico en la sociedad del futuro (Solemne Sesión Académica en Banja Luka celebrada el 16 de mayo de 2011), 2011.*

M25B/11 *Globalisation, governance and ethics: new managerial and economic insights (Edición Nova Science Publishers), 2011.*

M-26/12 *Decidir hoy para crear el futuro del Mediterráneo (VII acto internacional celebrado el 24 de noviembre de 2011), 2012.*

M-27/12 *El ciclo real vs. el ciclo financiero un analisis comparativo para el caso español. Seminario sobre política anticíclica, 2012.*

M-28/12 *Gobernando las economías europeas. La crisis financiera y sus retos. (Solemne Sesión Académica en Helsinki celebrada el 9 de febrero de 2012), 2012.*

M-29/12 *Pasado y futuro del área mediterránea: consideraciones sociales y económicas (Solemne Sesión Académica en Bejaia celebrada el 26 de abril de 2012), 2012.*

M-31/13 *Why austerity does not work: policies for equitable and sustainable growth in Spain and Europe (Conferencia del académico correspondiente para Estados Unidos, Excmo. Sr. Dr. D. Joseph E. Stiglitz, Pronunciada en Barcelona en diciembre de 2012), 2013.*

M-32/13 *Aspectos micro y macroeconómicos para sistemas sociales en transformación (Solemne Sesión Académica en Andorra celebrada el 19 de abril de 2013), 2013.*

M-33/13 *La unión europea más allá de la crisis (Solemne Sesión Académica en Suiza celebrada el 6 de junio de 2013), 2013.*

M-33B/13 *Decision Making Sytems in Business Administration (Proceedings de MS'12 International Conference celebrada en Río de Janeiro los días 10-13 de diciembre de 2012). Edición de World Scientific, 2013.*

M-34/14 *Efectos de la evolución de la inversión pública en Educación Superior. Un estudio del caso español y comparado (Trabajo presentado por la Sección Primera de la Real Academia de Ciencias Económicas y Financieras), 2014.*

M-35/14 *Mirando el futuro de la investigación científica (Solemne Acto Académico Conjunto celebrado en Bakú el 30 de mayo de 2014), 2014.*

M-36/14 *Decision Making and Knowledge Decision Support Systems (VIII International Conference de la RACEF celebrada en Barcelona e International Conference MS 2013 celebrada en Chania Creta. Noviembre de 2013). Edición a cargo de Springer, 2014.*

M-37/14 *Revolución, evolución e involución en el futuro de los sistemas sociales (IX Acto internacional celebrado el 11 de noviembre de 2014), 2014.*

M-39/15 *Nuevos horizontes científicos ante la incertidumbre de los escenarios futuros (Solemne Acto Académico Conjunto celebrado en Cuba el 5 de mayo de 2015), 2015.*

M-40/15 *Ciencia y realidades económicas: reto del mundo post-crisis a la actividad investigadora (X Acto Internacional celebrado el 18 de noviembre de 2015), 2015.*

ME-42/16 *Vivir juntos (Trabajo presentado por la Sección Tercera de la Real Academia de Ciencias Económicas y Financieras), 2016.*

MS-43/16 *¿Hacia dónde va la ciencia económica? (Solemne Acto Académico Conjunto con la Universidad Estatal de Bielorrusia, celebrado en Minsk el 16 de mayo de 2016), 2016.*

MS-44/16 *Perspectivas económicas frente al cambio social, financiero y empresarial(Solemne Acto Académico Conjunto con la Universidad de la Rioja y la Fundación San Millán de la Cogolla, celebrado en La Rioja el 14 de octubre de 2016), 2016.*

MS-45/16 *El Comportamiento de los actores económicos ante el reto del futuro (XI Acto Internacional de la Real Academia de Ciencias Económicas y Financieras, celebrado en Barcelona el 10 de noviembre de 2016), 2016.*

MS-46/17 *El agua en el mundo-El mundo del agua/ Water in the world- The World of Water (Nueva Edición Bilingüe Español-Inglés del Estudio a cargo del Prof. Dr. Jaime Lamo de Espinosa, publicada con motivo del 150 aniversario de Agbar), 2017.*

MS-48/17 *El pensamiento económico ante la variedad de espacios españoles (Solemne Acto Académico conjunto con la Universidad de Extremadura y la Junta de Extremadura celebrado los días 2-3 de marzo de 2017), 2017.*

MS-49/17 *La economía del futuro en Europa. Ciencia y realidad. Calmîc, Octavian; Aguer Hortal, Mario; Castillo, Antonio; Ramírez Sarrió, Dídac; Belostecinic, Grigore; Rodríguez Castellanos, Arturo; Bîrcă, Alic; Vaculovschi, Dorin; Metzeltin, Michael; Verejan, Oleg; Gil Aluja, Jaime.*

MS-51/17 *Las nuevas áreas del poder económico (XII Acto Internacional de la Real Academia de Ciencias Económicas y Financieras celebrado en Barcelona el 16 de noviembre de 2017), 2017.*

MS-53/18 *El reto de la prosperidad compartida. El papel de las tres culturas ante el siglo XXI. Solemne acto académico conjunto con la Fundación Tres Culturas del Mediterráneo (Barcelona Economics Network). Askenasy, Jean; Imanov, Gorkmaz; Granell Trias, Francesc; Metzeltin, Michael; Bernad González, Vanessa; El Bouyoussfi, Mounir; Ioan Franc, Valeriu; Gutu, Corneliu.*

MS-54/18 *Las ciencias económicas y financieras ante una sociedad en transformación. Solemne Acto Académico conjunto con la Universidad de León y la Junta de Castilla y León, celebrado el 19 y 20 de abril de 2018. Rodríguez Castellanos, Arturo; López González, Enrique; Escudero Barbero, Roberto; Pont Amenós, Antonio; Ulibarri Fernández, Adriana; Mallo Rodríguez, Carlos; Gil Aluja, Jaime.*

MV-01/18 *La ciencia y la cultura ante la incertidumbre de una sociedad en transformación (Acto Académico de la Real Academia de Ciencias Económicas y Financieras en la Universidad de Tel Aviv celebrado el 15 y 16 de mayo de 2018), 2018.*

MS-55/19 *Desafíos de la nueva sociedad sobrecompleja: Humanismo, dataísmo y otros ismos (XIII Acto Internacional de la Real Academia de Ciencias Económicas y Financieras celebrado en Barcelona el 15 y 16 de noviembre de 2018), 2018.*

MS-57/19 *Complejidad Financiera: Mutabilidad e Incertidumbre en Instituciones, Mercados y Productos. Solemne Acto Académico Conjunto entre la Universitat de les Illes Balears, la Real Academia de Ciencias Económicas y Financieras de España, el Cercle Financer de Balears, el Colegio de Economistas de las Islas Baleares y el Cercle d'Economia de Mallorca, celebrado los días 10-12 de abril de 2019. Rodríguez Castellanos, Arturo; López González, Enrique; Liern Carrión, Vicente; Gil Aluja, Jaime.*

ME-58/19 *Un ensayo humanista para la formalización económica. Bases y aplicaciones (Libro Sección Segunda de la Real Academia de Ciencias Económicas y Financieras), 2019.*

MS-59/19 *Complejidad Económica: Una península ibérica más unida para una Europa más fuerte. Solemne Acto Académico Conjunto entre la Universidad de Beira Interior – Portugal y la Real Academia de Ciencias Económicas y Financieras de España, celebrado el día 19 de junio de 2019. Askenasy, Jean; Gil Aluja, Jaime; Gusakov, Vladimir; Hernández Mogollón, Ricardo; Imanov, Korkmaz; Ioan-Franc, Valeriu; Laichoubi, Mohamed; López González, Enrique; Marino, Domenico; Redondo López, José Antonio; Rodríguez Rodríguez, Alfonso; Gil Lafuente, Ana Maria.*

MS-62/20 *Migraciones (XIV Acto Internacional de la Real Academia de Ciencias Económicas y Financieras celebrado en Barcelona el 14 y 15 de noviembre de 2019), 2019.*

MS-63/20 *Los confines de la equidad y desigualdad en la prosperidad compartida. Solemne Acto Académico Conjunto entre la Universidad de Cantabria y la Real Academia de Ciencias Económicas y Financieras, celebrado los días 7 y 8 de mayo de 2020. Ramírez Sarrió, Dídac; Gil Aluja, Jaime; Rodriguez Castellanos, Arturo; Gasòliba, Carles; Guillen, Montserrat; Casado, Fernando; Gil-Lafuente, Ana Maria, Sarabia Alegría, José María.*

MS-66/21 *La vejez: conocimiento, vivencia y experiencia (XV Acto Internacional de la Real Academia de Ciencias Económicas y Financieras celebrado en Barcelona el 10 y 20 de noviembre de 2020), 2020.*

MS-67/21 *Sistemas de pensiones para una longevidad creciente. Una mirada a los sistemas de pensiones en Bielorrusia, España, Finlandia, México y Suiza. Daniel i Gubert, Josep; Wanner, Jean-Marc; Gusakov, Vladimir; Kiander, Jaakko; González Santoyo, Federico; Flores Romero, Beatriz; Gil-Lafuente, Ana Maria; Guillen, Montserrat. 2021.*

MS-69/21 *Ciencia y actividad económica: propuestas y realidades (Trabajos correspondientes al I Ciclo de Conferencias Internas). Gil Aluja, Jaime; Granell Trias, Francesc; Aguer Hortal, Mario; Ramírez Sarrió, Dídac; Argandoña Rámiz, Antonio; Liern Carrión, Vicente; Gil-Lafuente, Ana María. 2021.*

MS-71/22 *Incidencias económicas de la pandemia. Problemas y oportunidades. Solemne Acto Académico Conjunto entre la Universidad de Valencia y la Real Academia de Ciencias Económicas y Financieras, celebrado los días 21 y 22 de octubre de 2021. Gil Aluja, Jaime; Aguer Hortal, Mario; Maqueda Lafuente, Francisco Javier; Ramírez Sarrió, Dídac; Liern Carrión, Vicente; Rodríguez Castellanos, Arturo; Guillén Estany, Montserrat.*

MS-72/22 *La nueva economía después del Sars-Cov-2. Realidades y revolución tecnológica. (XVI Acto Internacional de la Real Academia de Ciencias Económicas y Financieras celebrado en Barcelona el 18 y 19 de noviembre de 2021), 2021.*

ME-73/22 *El Banco Central Europeo y la crisis financiera (2007-2018). Sección de Ciencias Económicas de la Real Academia de Ciencias Económicas y Financieras. Argandoña Rámiz, Antonio; Castells Oliveres, Antoni. 2022.*

MS-74/22 *Ciencia y actividad económica: propuestas y realidades (Trabajos correspondientes al II Ciclo de Conferencias Internas). Gil Aluja, Jaime; Rodríguez Rodríguez, Alfonso; Guillén Estany, Montserrat; Rodríguez Castellanos, Arturo; Lago Peñas, Santiago; Barquero Cabrero, José Daniel; López González, Enrique. 2022.*

MS-75/22 *Soluciones económicas y tecnológicas a la degradación del ecosistema del planeta. (I Seminario Internacional Abierto de Barcelona de la Real Academia de Ciencias Económicas y Financieras celebrado en Barcelona el 8 y 9 de junio de 2022) ,2022.*

ME-76/22 *Economistas Españoles Relevantes de los siglos XVIII, XIX y XX. Real Academia de Ciencias Económicas y Financieras. Aguer Hortal, Mario. 2022.*

MS-77/23 ¿Por qué no un Mundo Sostenible? La Ciencia Económica va a su encuentro. *(XVII Acto Internacional de la Real Academia de Ciencias Económicas y Financieras celebrado en Barcelona el 16 y 17 de noviembre de 2022) ,2022.*

MS-78/23 *Los nuevos desafíos y oportunidades de la transformación digital de la economía española. (Solemne Acto Académico conjunto entre la Universidad de Salamanca y la Real Academia de Ciencias Económicas y Financieras celebrado en Salamanca el 15 de marzo de 2023) ,2023.*

MS-79/23 La Ciberseguridad como imperativo para la Economía de España. *(Solemne Acto Académico conjunto entre el Instituto Nacional de Ciberseguridad y la Real Academia de Ciencias Económicas y Financieras celebrado en León el 17 de marzo de 2023) , 2023.) ,2023.*

MS-81/23 Ciencia y actividad económica: propuestas y realidades *(Trabajos correspondientes al III Ciclo de Conferencias Internas). Gil Aluja, Jaime; Gasòliba Böhm, Carles-Alfred; Daniel i Gubert, Josep; Maqueda Lafuente, Francisco Javier; Terceño Gómez, Antonio; Lamo De Espinosa; Jaime. 2023.*

MS-85/24 La Ciberseguridad en la Ciencia y en las actividades económicas *(Trabajos correspondientes al II Seminario Internacional de primavera de Barcelona). Gil Aluja, Jaime; Petre Roman; Enrique Lecumberri Matí; Ana Maria Gil-Lafuente, Valeriu Ioan Franc; Korkmaz Imanov; Domenico Marino; Dobrica Milovanovic; Carlo Morabito; Enrique López; Jose Daniel Barquero; Janusz Kacprzyk; Mario Aguer. 2023.*

Los orígenes más remotos de la Real Academia de Ciencias Económicas y Financieras de España se remontan al siglo XVIII, cuando en 1758 se crea en Barcelona la Real Junta Particular de Comercio.

El espíritu inicial que la animaba entonces ha permanecido hasta nuestros días: el servicio a la sociedad, a partir del estudio y de la investigación., es decir, actuar desde la razón y desde el humanismo. De ahí las palabras que aparecen en su escudo y medalla: "Utraque Unum".

La forma actual de la Real Corporación tiene su gestación en la década de los años 30 del pasado siglo. Su recreación se produce el 16 de mayo de 1940. En 1958 adopta el nombre de Real Academia de Ciencias Económicas y Financieras. En el año 2017 se incorpora, con todos los honores, en la máxima representación científica española: el Instituto de España.

En estos últimos años se ha potenciado de tal manera la internacionalización de la Real Academia de Ciencias Económicas y Financieras de España que hoy es considerada la Real Academia con mayor número de convenios de Colaboración Científica de nuestro país.

Su alto prestigio se ha asentado, principalmente, en cuatro direcciones. La primera de ellas, es la incorporación de grandes personalidades del mundo académico y de la actividad económica de los estados y de las empresas, con seis Premios Nobel, cuatro ex Jefes de Estado y varios Primeros Ministros.

La segunda, es la realización anual de sesiones científicas en distintos países junto con altas instituciones académicas de otros Estados, con los que se han firmado acuerdos de colaboración.

En tercer lugar, se están elaborando trabajos de estudio y análisis sobre la situación y evolución de los sistemas económico-financieros de distintas Naciones, con gran repercusión, no sólo en los ámbitos propios de la formalización científica, sino también en la esfera de las relaciones económicas, empresariales e institucionales.

En cuarto lugar, su principal, aunque no exclusivo, ámbito de trabajo se ha focalizado en la búsqueda y hallazgo de una vía de investigación nueva en el campo económico desde sus mismas raíces, con objeto de incorporar, numéricamente, el inevitable grado o nivel de subjetividad del pensamiento y decisión de los humanos. Por ello, la Real Academia de Ciencias Económicas y Financieras es conocida mundialmente por cuanto sus componentes forman parte y protagonizan la llamada **Escuela de Economía Humanista de Barcelona**.

La inmortalidad académica, cobra, así, su más auténtico sentido.

Jaime Gil Aluja
Presidente de la Real Academia de Ciencias Económicas
y Financieras de España

ULTIMOS ACTOS INTERNACIONALES DE LA REAL ACADEMIA DE CIENCIAS ECONÓMICAS Y FINANCIERAS

VII ACTO INTERNACIONAL (24/11/2011)
"Decidir hoy para crear el futuro del Mediterráneo"

VIII ACTO INTERNACIONAL (5/11/2013)
"Ciencia, cultura y deporte en el Siglo XXI"

IX ACTO INTERNACIONAL (11/11/2014)
"Revolución, evolución e involución en el futuro de los sistemas sociales"

X ACTO INTERNACIONAL (18/11/2015)
"Ciencia y realidades económicas: reto del mundo post-crisis a la actividad investigadora"

XI ACTO INTERNACIONAL (10/11/2016)
"El comportamiento de los actores económicos ante el reto del futuro"

XII ACTO INTERNACIONAL (16/11/2017)
"Las nuevas áreas del poder económico mundial"

XIII ACTO INTERNACIONAL (15-16/11/2018)
"Desafíos de la nueva sociedad sobrecompleja: humanismo, transhumanismo, dataísmo i otros ismos"

XIV ACTO INTERNACIONAL (14-15/11/2019)
"Migraciones"

XV ACTO INTERNACIONAL (19-20/11/2020)
"La vejez: conocimiento, vivencia y experiencia"

XVI ACTO INTERNACIONAL (18-19/11/2021)
"La nueva economía después del Sars-Cov-2. Realidades y revolución tecnológica"

XVII ACTO INTERNACIONAL (16-17/11/2022)
"¿Por Qué no un mundo sostenible? La ciencia económica va a su encuentro."

II SEMINARIO INTERNACIONAL (24-25/5/2023)
"La Ciberseguridad en la Ciencia y en las Actividades Económicas"

Real Academia de Ciencias Económicas y Financieras

SEMINARIO INTERNACIONAL DE PRIMAVERA DE BARCELONA

MS-85/24

LA CIBERSEGURIDAD EN LA CIENCIA Y EN LAS ACTIVIDADES ECONÓMICAS

II Seminario Internacional de Primavera de Barcelona

La Real Academia de Ciencias Económicas y Financieras organiza cada año una serie de actos académicos internacionales en su sede de Barcelona con la participación de científicos, expertos y académicos de diferentes continentes. Este año 2023 se ha desarrollado el II Seminario Internacional de Primavera con plena normalidad. La presencia de participantes ha sido de las más elevadas, añadiéndose además numerosas participaciones virtuales.

Las aportaciones científicas realizadas por los ponentes se han centrado en torno a la cuestión que plantea la ciberseguridad en la ciencia y las actividades económicas haciendo especial hincapié en los profundos cambios estructurales, en ocasiones disruptivos, que ya se están produciendo y seguirán produciéndose en el futuro: nos referimos a los efectos económicos, por una parte; y a la revolución tecnológica como nuevo paradigma social, por otra.

El contenido de los trabajos aportados a esta conferencia internacional ha quedado recogido y publicado en una obra en forma de libro, así como en los distintos formatos digitales de los canales habituales.

La actividad científica y académica de la Real Academia de Ciencias Económicas y Financieras sigue su andadura siempre adaptándose a las vicisitudes del entorno y fiel al mandato que tiene encomendado en su tarea de investigar y difundir el conocimiento.

Real Academia de Ciencias Económicas y Financieras