Universidad de
SanAndrés

Universidad de San Andrés

Departamento de Ciencias Sociales

Licenciado en Relaciones Internacionales

Ciberseguridad y Política Internacional

Autor: Eduardo Brovchuk

Legajo: 31013

Mentor: Federico Merke

Buenos Aires, Argentina

26 de junio de 2023

Agradecimientos

En esta sección quiero agradecer a todos los que me ayudaron en mi carrera universitaria que termina con este trabajo de investigación. A mi familia y a mis amigos por estar en el día a día apoyándome de forma constante para poder llegar hasta acá. Y a todos los profesores de la Universidad de San Andrés, en especial a mi mentor Federico Merke, por su constancia y su dedicación diaria imprescindible para todos nosotros como alumnos.

A mi mama y a mi hermana, especialmente, por enseñarme que el valor del esfuerzo, la disciplina y la constancia tienen sus frutos a largo plazo

Abstract

En el presente trabajo, se analizan los factores que influyen en los niveles de ciberseguridad en los Estados. A través de datos de panel, obtenidos de diversas fuentes, y una regresión lineal se intenta precisar si el pbi pér capita, los niveles de democracia y los niveles de desarrollo de un gobierno digital afectan a los niveles de ciberseguridad. Los resultados corroboran que, por un lado, los niveles de democracia perjudican los niveles de ciberseguridad y, por otro lado, la existencia de una relación positiva entre el nivel de desarrollo de un gobierno digital y los niveles de ciberseguridad. Por último, afirmamos que no existe información suficiente para afirmar que el PBI per cápita tenga una relación directa con la ciberseguridad.

Introducción

La ciberseguridad se refiere a las medidas que se toman para la protección de las operaciones de un sistema computacional o de la integridad de sus datos ante acciones hostiles (Kello, 2013). A su vez, es un concepto que se puede concebir dentro de los asuntos del Estado como la infraestructura para su defensa en contra de ciber incidentes potencialmente maliciosos que traspasen sus fronteras a través de canales digitales (Valeriano y Maness, 2016). Por esta razón, la ciberseguridad es una problemática que amerita una reflexión debido al impacto que produce cada avance tecnológico en nuestra vida cotidiana, desde cómo nos comunicamos hasta cómo analizamos y procesamos la información. Este cambio continuo está interconectado al ámbito político y militar de los Estados, donde aparecen nuevas amenazas y percepciones de vulnerabilidad.

Ejemplos de estas nuevas amenazas son los detectados por la Organización Internacional de Policía Criminal (INTERPOL) en un informe sobre la ciberdelincuencia en agosto del año 2020. En dicho informe se muestra el aumento sistemático de diferentes tipos de cibercrímenes, como las estafas por internet, el phishing, los malwares disruptivos o los dominios malignos, debido a la pandemia del COVID-19. El contexto global de ese año funcionó como un amplificador de este tipo de amenazas, poniendo bajo presión a las fuerzas de seguridad de los Estados y, por ende, a su ciberseguridad.

Otro ejemplo que muestra la creciente importancia de esta temática es la estimación de la pérdida global de dinero realizada por McAfee, una de las empresas más importantes en lo que se refiere a la seguridad informática a nivel global, causada por el cibercrimen. Según sus estimaciones, estas pérdidas ascendieron a 1 trillón de dólares en el año 2020 y han alcanzado los 6 trillones de dólares en el año 2021. Estos datos nos brindan una razón adicional para comprender por qué la ciberseguridad se ha vuelto una problemática importante en una sociedad que avanza hacia la digitalización.

En el presente trabajo, se buscará analizar por qué varían los niveles de ciberseguridad en los Estados y qué elementos son esenciales para una política de ciberseguridad basada en evidencia. Para ello, se tomarán los ciento noventa y tres Estados miembro de Naciones Unidas como objeto de estudio. De esta manera, la pregunta principal que

guía esta investigación es *cuales son los factores que influyen en la variación de los niveles de ciberseguridad en los Estados*.

En primer lugar, se expondrá las principales ideas y debates en torno a la ciberseguridad. Esto llevará a distinguir el foco principal que ha tenido la literatura respecto a la problemática, es decir, el debate en torno a si los ciberataques podrían constituirse en actos de guerra o no. Sin embargo, la literatura carece de un análisis de cómo y por qué pueden variar los niveles de ciberseguridad. Con esta investigación se intentará realizar un aporte a un campo que se encuentra en constante evolución y crecimiento.

En segundo lugar, en esta sección se presentarán las variables de estudio junto con las hipótesis que guían el análisis.

Por un lado, se sugiere que los países desarrollados tienen altos índices de ciberseguridad debido a que el desarrollo de estrategias y de sistemas defensivos en el ciberespacio requiere de grandes inversiones que sólo los países con altos índices de PBI per cápita pueden realizar.

Por otro lado, se espera que los países democráticos tengan altos índices de ciberseguridad debido a que buscan proteger el proceso electoral que es uno de los elementos esenciales para el funcionamiento de las instituciones democráticas. La principal consecuencia de un ataque al proceso electoral es la desestabilización del régimen como se pudo ver en el año 2016 en las elecciones presidenciales de Estados Unidos.

Por último, se sugiere que los países con mayores índices de gobierno electrónico tienen mayores índices de ciberseguridad ya que en esos casos los Estados tienen mayor preparación, agilidad y adaptación ante las nuevas tecnologías por lo que les es más fácil contrarrestar una amenaza. Y, por lo tanto, no ser vulnerables a diferencia de otros países del orden internacional.

En tercer lugar, se dará a conocer la metodología utilizada para evaluar aquellas hipótesis. Cada hipótesis será evaluada a través de una base de datos diferente: PBI per cápita provista por el Banco Mundial, Liberal Democracy Index provisto por el instituto V-Dem y el Índice de Desarrollo del Gobierno Electrónico proporcionado por el Departamento de Asuntos Económicos y Sociales de las Naciones Unidas. Con las bases

de datos obtenidas se trabajará con datos de panel al tener tanto variaciones de tiempo como de países para poder ver las tendencias a través de tablas de regresión.

Para finalizar, se detallarán los resultados empíricos obtenidos para dar paso a las conclusiones de esta investigación que demuestra que los factores que influyen en los niveles de ciberseguridad son los niveles de democracia y los niveles de desarrollo de un gobierno digital. Por un lado, los niveles de democracia afectan de forma negativa a la ciberseguridad y, por otro lado, existe una relación positiva entre los niveles de desarrollo de un gobierno digital y los niveles de ciberseguridad. Con respecto al PBI per cápita, no existe información suficiente que permita afirmar que exista una relación directa entre el nivel de desarrollo económico y la ciberseguridad.

Revisión de la literatura

La ciberseguridad es un ámbito de estudio que ha tenido un crecimiento en su investigación y desarrollo en los últimos años. Los investigadores han abordado este tema desde diferentes perspectivas, y uno de los debates más relevantes se centra en si los ciberataques pueden constituirse en actos de guerra, es decir, si existe la posibilidad de una ciberguerra. En esta sección, se analizarán dos perspectivas opuestas sobre este debate.

La ciberguerra será posible

Por un lado, la primera perspectiva considera que los ciberataques pueden constituirse en actos de guerra. De hecho, los autores que defienden esta postura hablan de una guerra latente y próxima. "Esto implica que la ciberguerra puede llegar a ser tan devastadora como la que hasta hace poco tiempo se entendía como guerra convencional" (Domínguez, 2016, p. 19)

En primer lugar, los defensores de esta postura argumentan que pueden constituirse en actos de guerra ya que los ciberataques implican la aplicación de la fuerza con el fin de producir efectos violentos, aunque aclaran que estos efectos no necesariamente tienen que ser letales. De hecho, como indica Stone (2013), los ciberataques pueden generar efectos violentos que pueden causar daños materiales y, por lo tanto, se pueden considerar actos de guerra. Es importante destacar en este argumento que los ciberataques no han producido hasta la actualidad una pérdida de vidas humanas, a diferencia de las armas convencionales.

En segundo lugar, otros autores consideran que se pueden considerar actos de guerra porque hay una gran posibilidad de que puedan causar grandes daños económicos y materiales que pueden derivar en la pérdida de vidas humanas a través del ataque a las infraestructuras críticas de los Estados. Por ejemplo: un ataque a una central eléctrica vital que derive en consecuencias tales como el desabastecimiento de agua, la inviabilidad en los transportes, etc.

En tercer lugar, porque los Estados han comenzado en invertir en su Ciberseguridad, como lo han hecho Alemania, Reino Unido y Francia, según Guitton (2013). Esto se puede observar través de la puesta de recursos tanto económicos como de capital humano y en la evolución de las medidas legales. Un ejemplo de esto último es la elaboración del Manual de Tallín por parte de la OTAN en 2013 en donde se aborda la

seguridad del ciberespacio y los conflictos cibernéticos en el Derecho Internacional. De esta forma, los autores abogan por una cooperación internacional para limitar la amenaza y generar un consenso preciso para el abordaje sobre la problemática. "De lo que se trata es de que se alcance un consenso mundial sobre la materia del ciberespacio, y la ciberguerra, en particular partiendo de los conceptos básicos y consensuados de Ciberseguridad y Ciberdefensa" (Dominguez, 2016, p. 31)

La ciberguerra no será posible

Por otro lado, la segunda perspectiva sostiene que los ciberataques no constituyen actos de guerra.

En primer lugar, como indica Rid (2013), los ciberataques no cumplen las condiciones necesarias para ser considerados actos de guerra. Estos deben cumplir los siguientes criterios: ser potencialmente letales, ser instrumentales y tener un propósito político. Por un lado, cuando se refiere a la letalidad, se hace alusión a la violencia física que puede ocasionar la muerte. Por otro lado, la instrumentalidad implica que debe haber medios y un fin definido. El objetivo último en la guerra es lograr que el oponente se rinda, ya sea por voluntad propia o porque no tenga alternativa de defensa, lo cual se logra a través de medios estratégicos. Por último, el ciberataque debe tener una dimensión política, ya que la guerra es llevada a cabo por una entidad política con una voluntad determinada. Por eso es que, "Cyber "war" is not likely to serve as the final arbiter of competition in an anarchical world and so should not be considered in isolation from more traditional forms of political violence" (Gartzke, 2013, p. 42)

Además, lo que argumenta Rid (2013) en su texto "Cyber War Will Not Take Place" es que los ciberataques son actividades relacionadas al sabotaje, al espionaje y a la subversión. En otras palabras, esto quiere decir que los ciberataques pueden ir desde la destrucción técnica de sistemas militares o económicos (sabotaje), la penetración en el sistema del enemigo para obtener información vital (espionaje) hasta el debilitamiento de un orden o autoridad establecida (subversión) como lo realizo Anonymous en sus ataques contra el Kremlin en el contexto de la guerra ruso-ucraniana.

Kello (2013) también menciona que las nociones tradicionales de guerra enfrentan dificultades para conceptualizar los ciberataques como actos de guerra. Entre estas dificultades se encuentran la posibilidad de que los ciberataques no sean violentos, el incumplimiento de estándares básicos en términos del uso de la fuerza armada en cuanto

a alcance, intensidad y duración de un ataque, así como la falta de objetivos estratégicos claros por parte de los perpetradores de los ciberataques, como ocurrió en el caso de Estonia en 2007 y como menciona Rid (2013) en su texto. Según el autor, "The implications for international security are potentially serious: (…) a cyber event can occur that does not meet the traditional definition of war but that nevertheless elicits a reprisal of commensurate severity" (Kello, 2013, p. 26).

En segundo lugar, los ciberataques no se pueden considerar actos de guerra porque la evidencia empírica estudiada hasta el momento demuestra que la tasa de conflicto entre Estados rivales es baja. "Only 20 of the 120 active rival dyads engage in cyber conflict; furthermore, although the number of cyber incidents have been on the rise since 2001, the impact and severity of the incidents have remained constant and at a relatively low level." (Valeriano y Maness, 2018, p. 5).

Entonces, ¿cuál fue la razón para que los Estados hayan invertido en ciberseguridad si empíricamente se ha demostrado que la tasa de conflicto es baja? Guitton (2013) analiza esta cuestión en su texto, centrándose en tres Estados europeos que han realizado inversiones significativas en ciberseguridad: Francia, Alemania y Reino Unido. Según el autor, dos factores principales influyeron en las decisiones de los representantes de estos Estados: el factor del contexto y la falta de evidencia empírica, lo que generó una percepción de amenaza similar entre los responsables de formular políticas públicas y la ciudadanía.

En relación con el contexto, existen dos casos importantes en cuanto se refiere a la ciberseguridad. Por un lado, el caso de Estonia en mayo de 2007. Durante ese período, el país experimentó una serie de ciberataques dirigidos a sus principales bancos, medios de comunicación y organismos estatales. Estos ataques tuvieron consecuencias significativas paralizando la vida cotidiana de los ciudadanos durante varias semanas.

Esto sucedió luego de la decisión del gobierno estonio de trasladar el monumento del Soldado de Bronce de la capital del país a las afueras de la ciudad.

Esta decisión se sumó a una amplia difusión de noticias falsas que afirmaban que el gobierno de Estonia planeaba destruir el monumento, así como las tumbas de guerra soviéticas. La controversia en torno al monumento generó tensiones y divisiones significativas dentro de la ciudadanía estonia. Por un lado, los rusoparlantes consideraban que el monumento representaba el sacrificio de los soldados soviéticos en la victoria sobre los nazis, mientras que algunos estonios lo veían como un recordatorio de la ocupación soviética de su tierra. Estas diferencias llevaron a fuertes protestas y

disturbios que se extendieron durante dos días. El gobierno estonio acusó al gobierno ruso de ser el autor de estos ataques, mientras que Moscú negó repetidamente cualquier implicación en los mismos.

"Placed in a European context, it is fair to assume that the attacks influenced the French and British perception of cyber threats. They caught up with policy measures started by their German by raising the threat to national security level." (Guitton, 2013, p. 24). Por esta razón es que en varios medios de comunicación el caso de Estonia se considera como la primera ciberguerra en la red.

Otro caso similar que puso en alerta a los Estados fue el de Stuxnet, el ciber incidente más sofisticado jamás lanzado (Valeriano y Maness, 2018). Este fue un virus informático descubierto en 2010 en las centrifugadoras de enriquecimiento de uranio de la planta Natanz en Irán programado para destruirlas e incluso con la capacidad de anular los interruptores de apagado de emergencia. Fue la primera vez que un ciberataque logró penetrar de forma inadvertida en una infraestructura crítica como lo es una planta nuclear. Varios expertos indican que, por la sofisticación del virus, fue diseñado por Estados Unidos e Israel para detener el programa de enriquecimiento de uranio de Irán, pero al igual que en el caso de Estonia no se comprobaron tales acusaciones.

En consecuencia, la percepción de amenaza producida por el contexto y la falta de investigación empírica en cuanto a la magnitud y frecuencia de los ciberataques llevó a estos Estados a tomar medidas proactivas en materia de ciberseguridad para prevenir, mitigar e investigar estas amenazas.

Como se puede observar en estos casos históricos importantes respecto a la ciberseguridad existe un desafío respecto a determinar con certeza quién está detrás de un ciberataque. Este es el problema de la atribución del cual se expondrá a continuación.

El problema de la atribución

El problema de la atribución es la dificultad que existe para atribuir de forma clara y precisa la responsabilidad de un ciberataque a un actor específico. Este problema complica la adopción de medidas legales o de retaliación si el Estado decide defenderse en respuesta a un ciberataque.

Según Rid y Buchanan (2015) la atribución se enfrenta a tres limitaciones para poder ser determinada: la inversión de recursos, tiempo y la sofisticación del adversario. Los

autores en su texto argumentan que es posible realizar la atribución, pero requiere de entrenamiento y liderazgo. Además, exponen que es una decisión política realizar una investigación sobre la atribución y que depende de lo que este en juego en el contexto producido por un ciberataque. “The more severe the consequences of a specific incident, and the higher its damage, the more resources and political capital will a government invest in identifying the perpetrators” (Rid y Buchanan, 2015, p. 27)

Metodología

Como se pudo observar anteriormente, la literatura se encuentra enfocada en el debate respecto a si los ciberataques pueden constituir actos de guerra. Sin embargo, lo que no se ha trabajado hasta el momento es en el cómo y por qué varían los niveles de ciberseguridad en el orden internacional. Por ello, el objetivo de este trabajo es poder entender los factores que generan cambios en aquellos niveles.

Las variables de estudio fueron obtenidas a través del análisis del Índice de Ciberseguridad Global provisto por la Unión de Telecomunicaciones, el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación. Allí se evalúan cinco pilares necesarios para poner en marcha la agenda de ciberseguridad a nivel internacional. Estos son:

1) Pilar legal: se refiere a la existencia de instituciones y marcos legales que permitan combatir el cibercrimen.
2) Pilar técnico: se refiere al desarrollo y a la capacidad tecnológica de un Estado para poder defenderse ante ciberataques.
3) Pilar organizativo: se refiere a la capacidad de coordinación y puesta en marcha de políticas públicas de ciberseguridad a nivel nacional.
4) Pilar de capacitación: se refiere a la existencia de investigación y desarrollo de la ciberseguridad, a los programas de educación y de entrenamiento de capital humano y su consecuente certificación
5) Pilar de cooperación: se refiere a la cooperación bilateral y multilateral tanto entre sectores públicos como privados

De estos pilares necesarios para poder desarrollar una política de ciberseguridad se desprenden las siguientes hipótesis.

En primer lugar, podemos suponer que los países desarrollados tienen altos índices de ciberseguridad porque pueden adquirir herramientas y una infraestructura de seguridad más sofisticada y mejor preparada. A su vez, pueden atraer expertos en el campo y desarrollar programas de educación y de entrenamiento que les permita investigar y poner en marcha sistemas de defensa más sólidos. Además, en los países desarrollados hay mayor probabilidad de que exista una colaboración entre el sector público y el sector privado para compartir prácticas e información y combatir en conjunto las amenazas cibernéticas. Entonces, la primera hipótesis es:

H1: Los países desarrollados tienen mayores índices de ciberseguridad

En segundo lugar, podemos suponer que los países democráticos son los que tienen mayores índices de ciberseguridad por la existencia del Estado de Derecho, es decir, estos Estados tienen un marco legal, claro y preciso sobre cómo abordar los delitos cibernéticos, perseguir a quienes los realizan y proteger los derechos de los ciudadanos en el ciberespacio. A su vez, dentro de los países democráticos también existe mayor probabilidad de una colaboración entre el sector público, el sector privado y la sociedad civil para el combate de las amenazas y la concientización sobre la protección de datos de cada uno de los ciudadanos. Por lo tanto, la segunda hipótesis es:

H2: Los países democráticos tienen mayores índices de ciberseguridad

En tercer lugar, podemos suponer que los países que tienen un mayor desarrollo de gobierno digital presentan mayores índices de ciberseguridad debido a que para poder ofrecer y facilitar los servicios públicos a la ciudadanía a través de la promoción de la información y la agilización de trámites burocráticos, por medio de las tecnologías de la información, se necesita un sistema de defensa preparado y efectivo para poder lograr los objetivos de un e-government. Por ello es que:

H3: Los países con mayor desarrollo de un gobierno digital tienen mayores índices de ciberseguridad

Los datos utilizados fueron recolectados de diferentes bases resumidas en esta tabla:

Hipótesis	Variable independiente	Indicador	Fuente
H1: existe una relación positiva entre desarrollo económico y la ciberseguridad	Nivel de desarrollo económico	PBI pér cápita	Banco Mundial
H2: existe una relación positiva entre democracia y la ciberseguridad	Tipo de régimen político	Liberal Democracy index	Varities of Democracy (V-Dem)

H3: existe una relación positiva entre el desarrollo de un gobierno digital y la ciberseguridad	Nivel de Desarrollo de un gobierno digital	E-Government Development Index	Departamento de Asuntos Económicos y Sociales de la ONU

Fuente: elaboración propia (Brovchuk, 2023)

Como se trabajará con datos de panel al tener variaciones de tiempo y de países se seleccionaron los años 2014, 2016, 2018 y 2020 ya que son los años de estudio del Índice de Ciberseguridad Global que además es la forma de medir la variable dependiente de nuestra investigación.

A excepción del PBI pér cápita, tanto la variable dependiente como las variables independientes fueron operacionalizadas de 0 a 1 donde 0 indica menor nivel de ciberseguridad, menor nivel de democracia liberal, menor nivel de desarrollo de gobierno digital y 1 indica mayor nivel de ciberseguridad, mayor nivel de democracia y mayor nivel de desarrollo gobierno digital.

Modelo

De esta manera, analizaremos los datos a través del diseño de un modelo lineal que se resume de la siguiente manera:

Factores que afecten el nivel de ciberseguridad = $\beta_0 + \beta_1$ PBI+ β_2 LDI + β_3 EG + ε

Resultados

En esta sección analizaremos los resultados obtenidos luego de haber explicitado el modelo puesto en práctica.

En primer lugar, observaremos los resultados en la tabla de regresión

Determinantes de la ciberseguridad

	Dependent variable:
	¿que hace variar la ciberseguridad?
PBI	0.000001
	(0.000001)
EG	1.1262***
	(0.0546)
LDI	-0.1489***
	(0.0429)
Constant	-0.0987***
	(0.0264)
Observations	496
R^2	0.6328
Adjusted R^2	0.6306
Residual Std. Error	0.1882 (df = 492)
F Statistic	282.6479*** (df = 3; 492)
Note:	*p<0.05; **p<0.01; ***p<0.001

En primer lugar, vemos que no tenemos información suficiente para afirmar que el PBI per cápita afecte a los niveles de ciberseguridad ya que no es estadísticamente significativa.

En segundo lugar, hallamos que la tercera hipótesis es válida ya que es estadísticamente significativa y positiva, por ende, es posible afirmar que los países que tienen un mayor desarrollo de un gobierno digital presentan niveles más altos de ciberseguridad.

Por último, observamos que el nivel de democracia está negativamente asociado a los niveles de ciberseguridad porque es estadísticamente significativa. Esto quiere decir que el nivel de democracia perjudica a los niveles de ciberseguridad.

Discusión

Los resultados obtenidos muestran diferentes cuestiones a destacar. Por un lado, no se halló suficiente información que sustente la relación positiva entre el desarrollo económico y los niveles de ciberseguridad de un Estado. Esto puede deberse a diversos motivos entre ellos que el Estado tenga otras prioridades como en sectores de salud o educación en donde debe invertir sus recursos limitados o por falta de conocimiento y experiencia en el campo. No necesariamente tiene que haber una relación directa ya que la capacidad económica de un país no constituye ni garantiza un alto grado de desarrollo en su ciberseguridad.

Por otro lado, los resultados avalan la tercera hipótesis y cobra sentido ya que uno de los principales objetivos de un e-government, es decir, de un gobierno digital es el uso de las tecnologías de información para promover un mayor acceso e inclusión a la ciudadanía y aquello incluye a la ciberseguridad. No es posible pensar el uso de las tecnologías para la agilización de trámites burocráticos, la facilitación en la comunicación entre el sector público, el sector privado y la sociedad civil y su participación política sin un sistema que pueda contrarrestar amenazas y vulnerabilidades existentes en el ciberespacio.

Sin embargo, resultó particularmente interesante como el nivel de democracia tiene una relación negativa con los niveles de ciberseguridad. Puede parecer contraintuitivo, pero cobra sentido al ver el retroceso de los niveles de democracia expuesto por los reportes del instituto del V-Dem o Varities of Democracy posteriormente acelerado por la pandemia del COVID-19. Allí se expone que el mundo se encuentra ante una ola de autocratización a nivel global que produjo que en la actualidad los niveles de democracia a nivel global se encuentren en los mismos niveles que a fines de los años 80.

A su vez, esto podría indicar que las autocracias pueden tener ciertas ventajas para poder obtener altos niveles de ciberseguridad. En primer lugar, porque el proceso de toma de decisiones se encuentra en una persona o en un grupo reducido que puede permitir la implementación de políticas de ciberseguridad de forma más rápida y coordinada ya que no necesita extensos debates y revisiones de presupuestos. En segundo lugar, las autocracias pueden llegar a tener mayor control y vigilancia de su población y eso incluye su infraestructura digital. Eso puede permitir que el control de

las ciber amenazas sea más efectivo. En tercer lugar, si una autocracia pone dentro de sus prioridades la ciberseguridad tiene una facilidad de relocalización de recursos que la democracia no tiene y que puede generar una percepción de desarrollo de las capacidades cibernéticas más fuerte. Es importante tener en cuenta que el costo es la innumerable cantidad de violaciones a los derechos humanos que esto conlleva como lo es la violación al derecho de la privacidad.

China es un ejemplo de lo mencionado anteriormente. Es un país que ha logrado un alto grado de ciberseguridad, pero a través de la censura dentro de las redes sociales e internet que se puede ver en las etiquetas de localización. Cuando un usuario realiza una publicación o un comentario en las redes sociales por debajo se especifica su ubicación de forma automática. Por ello se debería trabajar en futuras investigaciones de forma específica la relación entre el tipo de régimen político y la ciberseguridad.

Conclusión

En conclusión, esta investigación obtuvo evidencia empírica que permite afirmar, en primer lugar, que el PBI per cápita no es un factor que influya en los niveles de ciberseguridad ya que la capacidad económica de un país no constituye ni garantiza un alto grado de desarrollo en su ciberseguridad.

En segundo lugar, que existe una relación negativa entre los niveles de democracia y los niveles de ciberseguridad. Esto puede relacionarse a la ola de autocratización que el mundo vive actualmente como lo ha expuesto el instituto del V-Dem en sus diferentes reportes o a las ventajas que posee una autocracia para poder llevar a cabo políticas de ciberseguridad más eficientes que van desde la rápida relocalización de recursos hasta el control y vigilancia que pueden llegar a tener sobre la población.

Por último, en tercer lugar, se comprobó que la tercera hipótesis es válida: existe una relación positiva entre los niveles de desarrollo de un gobierno digital y los niveles de ciberseguridad. Esto es importante ya que demuestra que, en la base del uso de las tecnologías de información por parte de un gobierno para el acceso, la inclusión y la participación de los ciudadanos se encuentra la ciberseguridad que permite tener herramientas para enfrentar amenazas existentes en el ciberespacio.

Bibliografía

Affairs, D. O. E. A. S. (2022). United Nations E-Government Survey 2022: The Future of Digital Government. United Nations.

Demchak, C. C., & Dombrowski, P. (2011). Rise of a Cybered Westphalian Age. *Strategic studies quarterly*, *5*(1), 32–61. http://www.jstor.org/stable/26270509

Domínguez, J. (2016). La ciberguerra como realidad posible contemplada desde la prospectiva. *Revista de Pensamiento Estratégico y Seguridad CISDE, 1(1)*, 18–32.

Fernmelde-Union, I. (2015). Global Cybersecurity Index 2014.

Fernmelde-Union, I. (2017). Global Cybersecurity Index 2016.

Fernmelde-Union, I. (2019). Global Cybersecurity Index 2018.

Fernmelde-Union, I. (2021). Global Cybersecurity Index 2020.

Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security*, *38*(2), 41–73. https://doi.org/10.1162/isec_a_00136

Guitton, C. (2013). Cyber insecurity as a national threat: overreaction from Germany, France and the UK? *European Security*, *22*(1), 21–35. https://doi.org/10.1080/09662839.2012.749864

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, *38*(2), 7–40. https://doi.org/10.1162/isec_a_00138

Maness, R. C., & Valeriano, B. (2016). The impact of cyber conflict on international interactions. *Armed Forces and Society*, *42*(2), 301–323. https://doi.org/10.1177/0095327x15572997

Möllers, N. (2021). Making digital territory: Cybersecurity, techno-nationalism, and the moral boundaries of the state. *Science, Technology & Human Values*, *46*(1), 112–138. https://doi.org/10.1177/0162243920904436

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of strategic studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Stone, J. (2013). Cyber War Will Take Place! *Journal of strategic studies*, *36*(1), 101–108. https://doi.org/10.1080/01402390.2012.730485

Tidy, J. (17 de marzo de 2022). Anonymous: "Intensificaremos los ataques contra el Kremlin". BBC. Recuperado el 26 de junio de https://www.bbc.com/mundo/noticias-internacional-60781082

Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19. (4 de agosto de 2020). *Interpol*. Recuperado el 26 de junio de 2023, de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research*, *51*(3), 347–360. https://doi.org/10.1177/0022343313518940

Valeriano, B., & Maness, R. C. (2018). International Relations theory and cyber security: Threats, conflicts, and ethics in an emergent domain. En C. Brown & R. Eckersley (Eds.), *The Oxford Handbook of International Political Theory*, 258–272. Oxford University Press.

V-Dem (2017). Democracy at Dusk? V-Dem Annual Report 2017, V-Dem Institute, Recuperado el 26 de junio de https://v-dem.net/documents/18/dr_2017.pdf

V-Dem (2019). Democracy Facing Global Challenges V-Dem Annual Report 2019, V-Dem Institute, Recuperado el 26 de junio de https://v-dem.net/documents/16/dr_2019_CoXPbb1.pdf

V-Dem (2021). Autocratizacion Turns Viral V-Dem Annual Report 2021, V-Dem Institute, Recuperado el 26 de junio de https://v-dem.net/documents/12/dr_2021.pdf