XXV Conferencia de Directores de Colegios de Defensa Iberoamericanos

XIII SEMINARIO ONLINE

El uso del espectro electromagnético y del ciberespacio en la seguridad nacional: la visión de los Colegios de Defensa Iberoamericanos

Ponencia:

Los desafíos y oportunidades del ciberespacio para la seguridad Nacional de los Estado-Nación Iberoamericanos

Dr. Edgar Ortiz Arellano
(CODENAL)

GOBIERNO DE MÉXICO

2024 AÑO DE Felipe Carrillo PUERTO
BENEMÉRITO DEL PROLETARIADO, REVOLUCIONARIO Y DEFENSOR DEL MAYAB

Introducción.

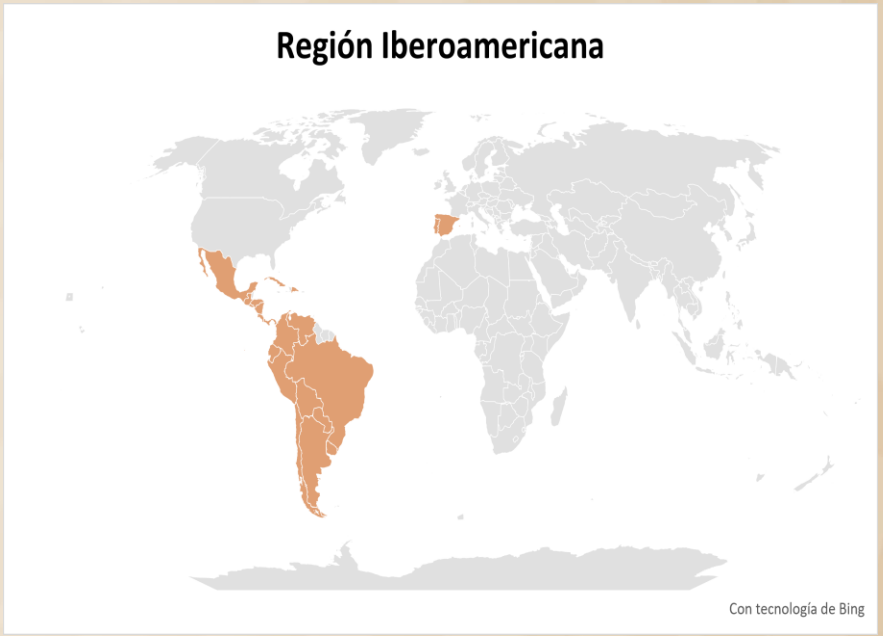
Los retos, amenazas y oportunidades que tienen los Estados Nación de Iberoamérica en la actualidad son diversos, complejos, pero el campo tecnológico y en especial el ciberespacio representan en muchas ocasiones una *terra incógnita* debido al desarrollo asimétrico que este ha tenido en algunos países iberoamericanos con respecto al centro del sistema-mundo.

El objetivo de esta ponencia es presentar un panorama general de las implicaciones que representa el ciberespacio en la seguridad nacional de la región iberoamericana, sus retos y oportunidades.

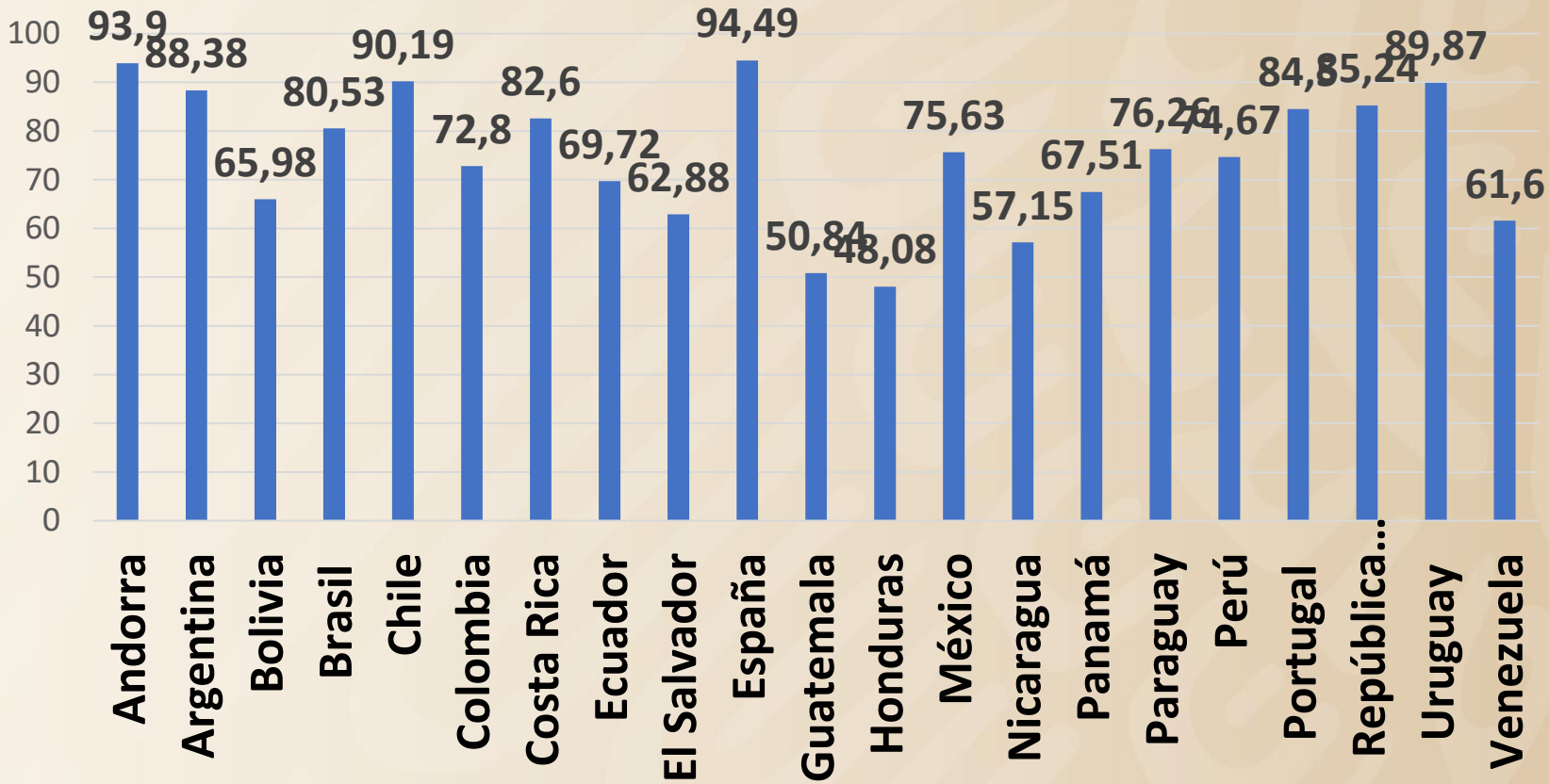
Contexto.

Iberoamérica es una de las regiones más dinámicas del mundo, su economía, población, bono democrático, recursos naturales y extensión territorial, la pueden proyectar como el epicentro del mundo en las próximas décadas, pero antes deberá resolver una serie de temas especialmente vinculados a la tecnología, la seguridad y el desarrollo equitativo de sus sociedades.

- 22 países
- Casi 700 millones de habitantes
- 20,591,128 de Km2 de territorio
- 10% PIB Global



Porcentaje de población con acceso a Internet en Iberoamérica



Fuente: World Economics (2023). Elaboración propia.

Datos Generales.

La cobertura mundial de población con acceso a internet en el año 2021 era del 62.6 por ciento.

La media de Iberoamérica de población con acceso a internet es de 75 por ciento. La región está por encima de la media mundial.

La media de latinoamérica de población con acceso a internet es de 72 por ciento. La región está por encima de la media mundial.

Las amenazas y oportunidades que se gestán en el ciberespacio se encuentran en el marco de la lucha de las potencias globales por la hegemonía mundial y la competencia por el acaparimiento de los mercados.

Los delitos cibernéticos a partir de la pandemia de Covid-19 aumentaron un 600 por ciento (Gutiérrez, 2022).

El 93 por ciento del malware es polimórfico (Gutiérrez, 2022).

Ciberseguridad y Futuro.

En la actualidad los responsables de la seguridad de los Estados deben de anticipar con precisión las tendencias a las que se enfrentan, una de ellas es la creciente digitalización y automatización de todos los ámbitos de la vida, muchos procesos de la vida moderna serían imposibles sin el soporte digital (Zdzikot, 2022).

Esto conlleva una dependencia de la tecnología y en particular de los fenómenos que se generan en el ciberespacio, debido a que ahí donde hay muchos procesos necesarios para la sociedad, por ejemplo, las transacciones financieras a gran escala o minoristas, control de los sistemas educativos y de salud, administración de infraestructura crítica del Estado-Nación; entre otras.

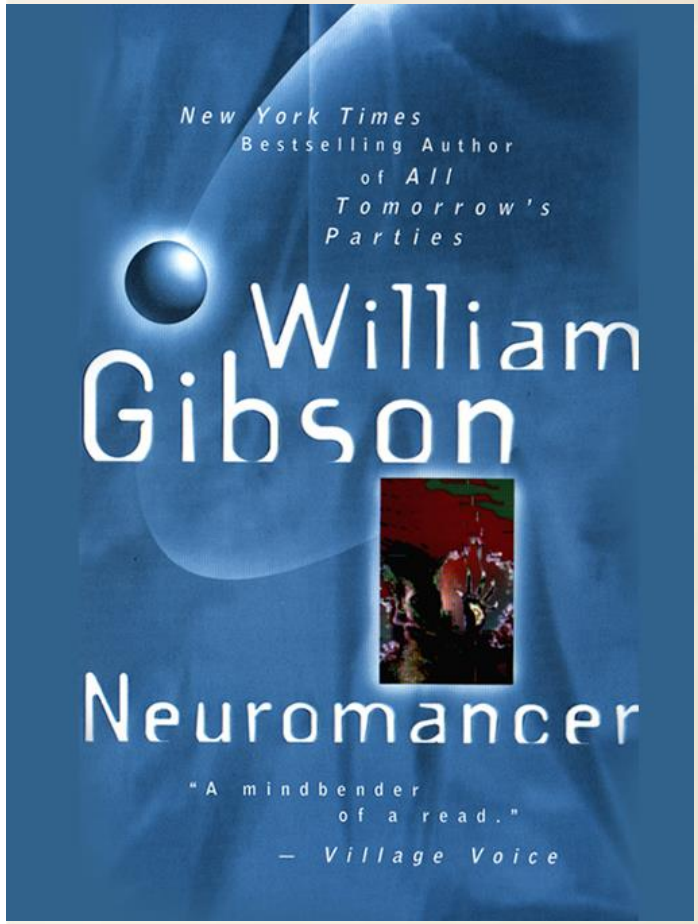
Daniel Bell, en su influyente libro *The Coming of Post Industrial Society* (1976), argumentó que las sociedades capitalistas avanzadas estaban pasando de la producción industrial a una economía basada en el conocimiento. Bell sugirió que, en esta nueva era, el conocimiento y la información reemplazarían al capital y al trabajo como principales fuentes de riqueza, poder y organización social (Mohseni, 2023: p. 50).

La actividad humana se está trasladando a la web, y el acceso a la información y el mantenerse constantemente "en contacto" se han convertido, en muchas esferas, en los determinantes básicos del éxito individual y organizacional. Al mismo tiempo, la facilidad de acceso a la información, así como a las tecnologías que permiten su generación y difusión, contribuye a un aumento constante de la oferta de datos (Zdzikot, 2022).

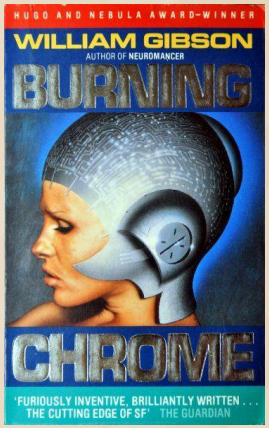
El ciberespacio dejó de ser un futuro de ficción para convertirse en un presente que ya no es influido por el mundo material, al contrario, se apropia de la materialidad y la moldea, en muchas ocasiones de manera distópica, de ahí que sea un tema estratégico para las áreas encargadas de la seguridad nacional

"[...] la matriz de ciberespacio era en realidad una drástica simplificación del sensorio humano, [...]" (Neuromante, 1984).

El ciberespacio como vocablo y concepto nace en la literatura, con las novelas Burning Chrome (1982) y Neuromancer de Gibson (1984), y es acogida por la informática, dado el parecido de la obra con lo que sucede en el mundo actual y las redes de ordenadores de distintos tipos sustentadas en la internet.

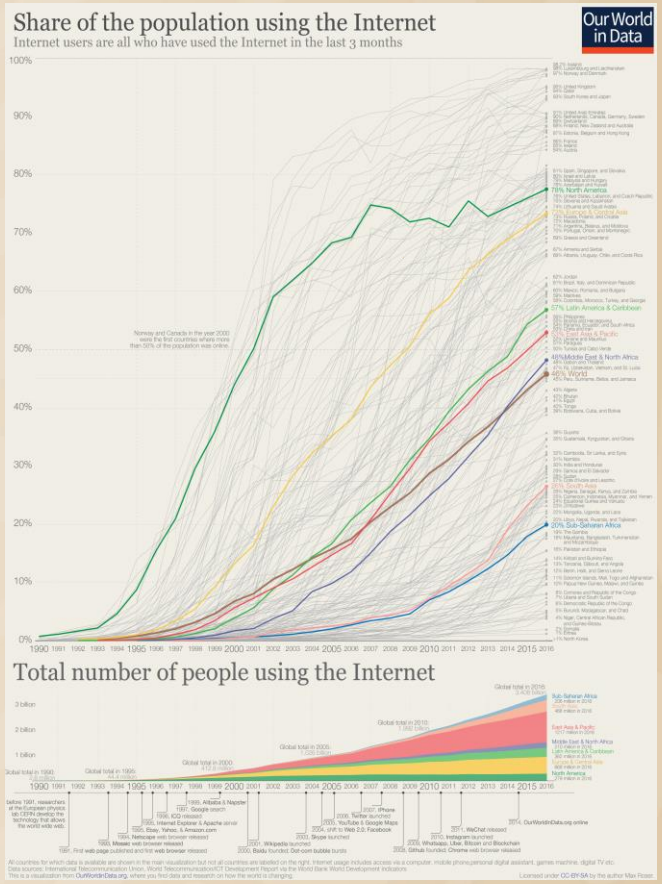


Ciberespacio como un espacio artificial y ficcional emergente en el que tienen lugar relaciones sociales entre personas, organizaciones y máquinas, y que no tiene existencia independiente del conjunto de equipos y programas informáticos que le posibilitan (Santana-Soriano y Báez, 2022: p. 49)



Ciberespacio:

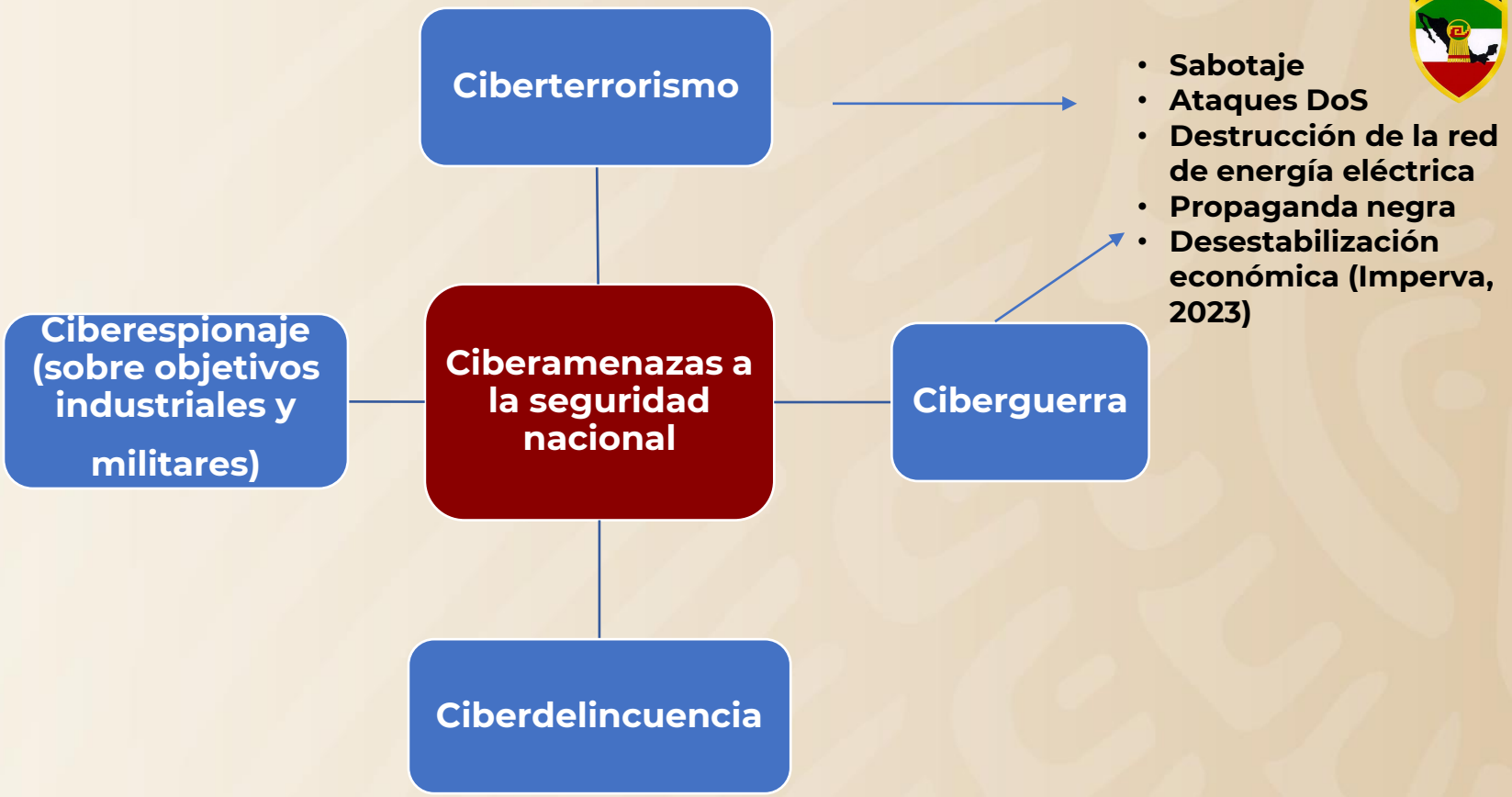
Entorno o ámbito intangible de naturaleza global, soportado por las Tecnologías de la Información y Comunicaciones, en el que se comunican e interactúan las entidades públicas, privadas y la sociedad en general, coadyuvando al desarrollo nacional y garantizando el ejercicio de los derechos y libertades como en el mundo físico (SEDENA-MARINA, 2021: p. 6).

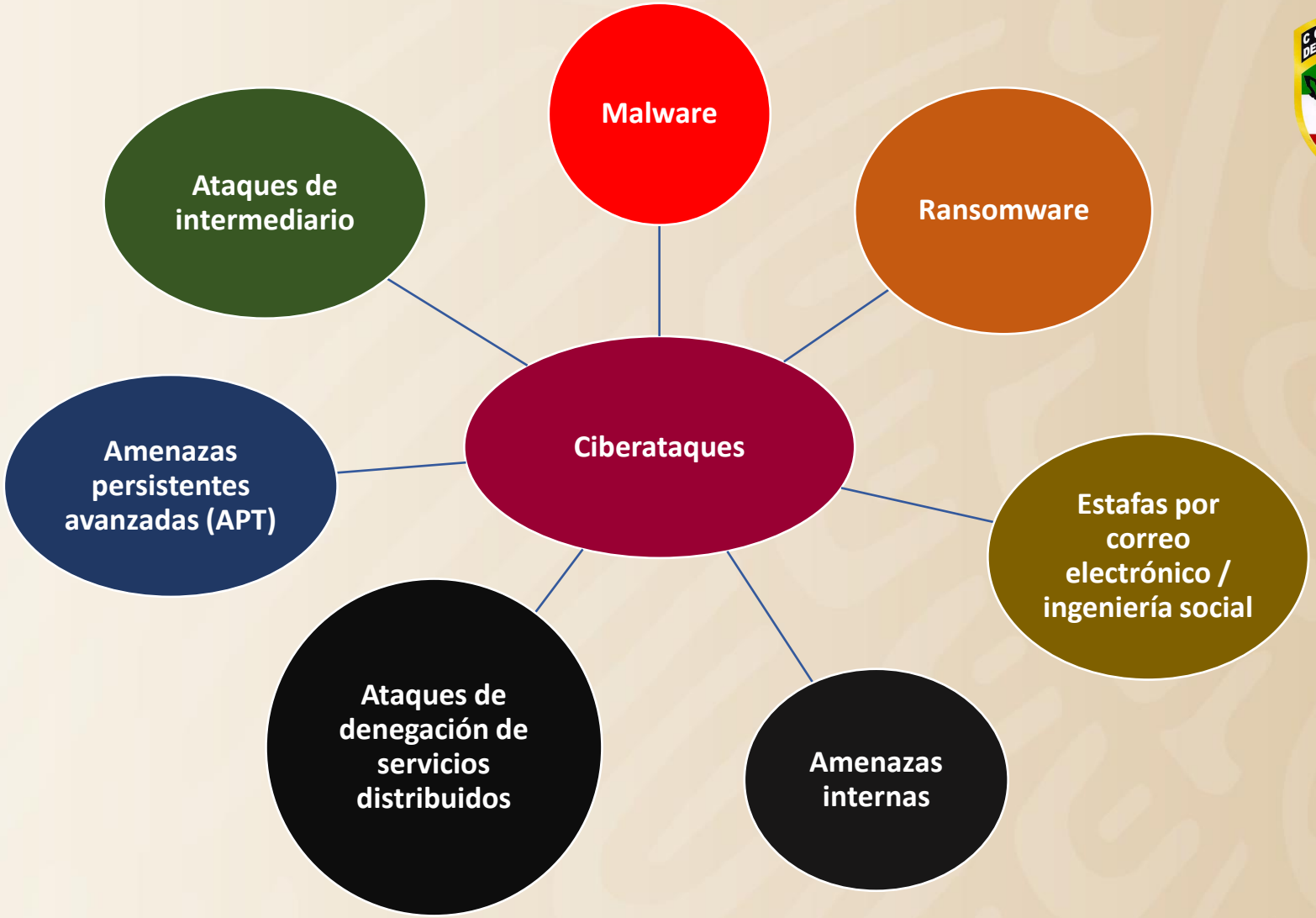


Ciberespacio es un dominio operativo ubicado simultáneamente en las capas lógica y física cuya arquitectura única está enmarcada por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de redes interconectadas que se cruzan perfectamente con otros dominios, así como con las fronteras políticas y geográficas (Mudrinich, 2012 en O´Brien, 2021).

El Desafío del Ciberespacio.

El ciberespacio tiene capas tanto lógicas como físicas. Esto significa que el ciberespacio puede ser utilizado como arma (es decir, la información puede usarse para causar daño físico) o como objetivo (es decir, la infraestructura física asociada con el dominio puede resultar dañada) por un terrorista u organización (O'Brien, 2021).


Ciberterrorismo
Ciberespionaje (sobre objetivos industriales y militares)
Ciberamenazas a la seguridad nacional
Ciberguerra
Ciberdelincuencia
• Sabotaje
• Ataques DoS
• Destrucción de la red de energía eléctrica
• Propaganda negra
• Desestabilización económica (Imperva, 2023)


Malware
Ataques de intermediario
Ransomware
Amenazas persistentes avanzadas (APT)
Ciberataques
Estafas por correo electrónico / ingeniería social
Ataques de denegación de servicios distribuidos
Amenazas internas

Extorsión Ransomware

El acoso es otra táctica de extorsión que también se utiliza cada vez en más casos de ransomware. Los grupos de ransomware se centran en determinadas personas de la organización, a menudo cargos ejecutivos, con amenazas y comunicaciones no deseadas. A finales de 2022 el acoso era un factor en cerca del 20 % de los casos de ransomware.

Es una práctica dirigida tanto a organismos públicos como privados (empresas y ONG´S)

Los atacantes a menudo amenazan con difundir los datos robados en sitios de filtraciones de la dark web, que cada vez juegan un papel más importante a la hora de extorsionar a las organizaciones

El sector de la fabricación industrial fue uno de los que sufrieron más ataques en 2022, con 447 organizaciones expuestas públicamente en sitios de filtraciones.

Según Unit 42 los países más afectados por intentos de extorsión de iberoamérica son Brasil, México, España y Argentina. A nivel mundial EE.UU es el país más afectado, seguido de Reino Unido, Alemania y Cánada.

Los grupos que utilizan amenazas avanzadas persistentes pueden utilizar la extorsión y el ransomware para financiar (u ocultar) otras actividades. Se han detectado grupos organizados de países sometidos a embargos o sanciones económicas que utilizan el ransomware y la extorsión para financiar sus operaciones.

Fuente: Unit 42 (2023)

Differences Between Regions

Top 5 cyber threats

All Regions

1. Clickjacking
2. Business Email Compromise (BEC)
2. Ransomware
4. Fileless Attack
5. Botnets

North America

1. Fileless Attack
2. Man-in-the-Middle Attack
3. Malicious Insiders
4. Business Email Compromise (BEC)
5. Watering Hole Attacks

Latin/South America

1. Clickjacking
2. Fileless Attack
3. Business Email Compromise (BEC)
3. Login Attacks (Credential Theft)
3. Ransomware

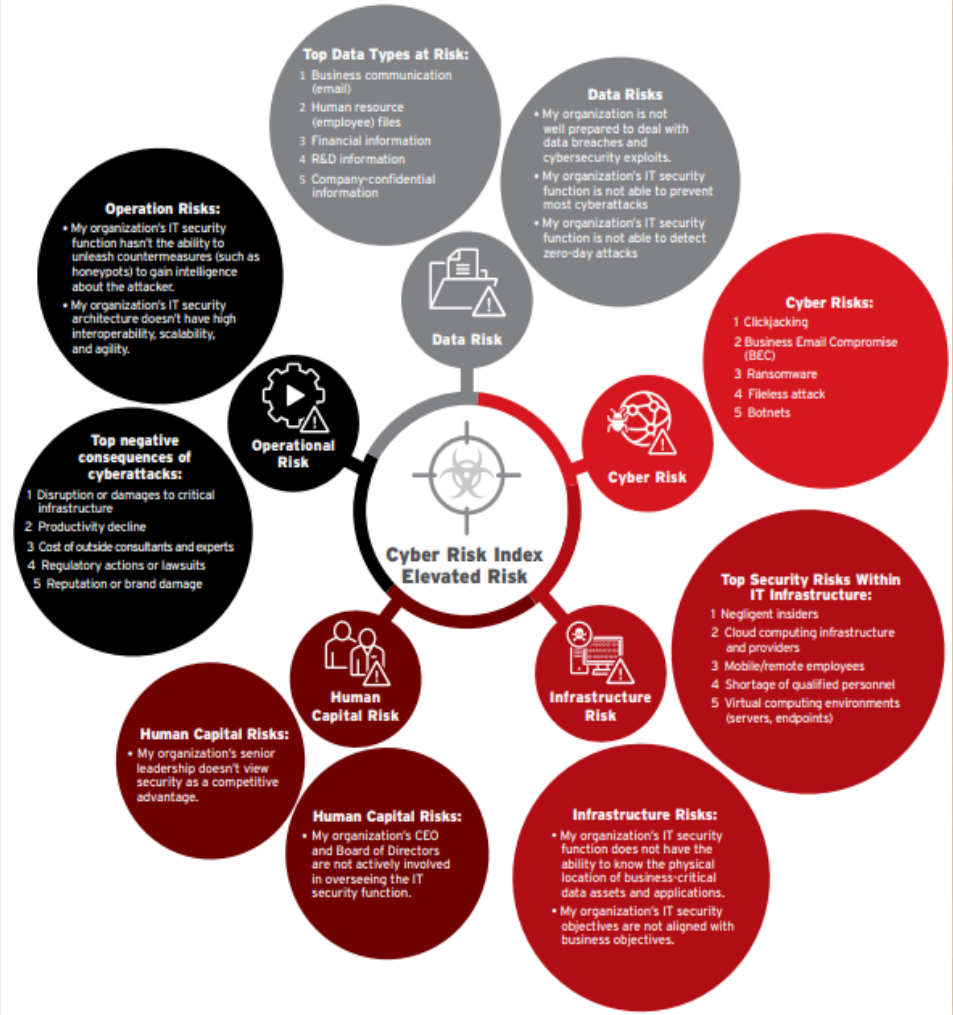
Europe

1. Clickjacking
2. Login Attacks (Credential Theft)
3. Ransomware
4. Botnets
5. Crypto Mining

Asia-Pacific

1. Business Email Compromise (BEC)
2. Ransomware
3. Clickjacking
4. Botnets
5. Crypto Mining

Fuente: Cyber Risk Index 2023



Fuente: Cyber Risk Index 2023

Grupos que perpetran ciberdelitos.

Ajax Security Team

Conti y REvil

APT39

Vice Society

BlackCat

Dragonfly

Carbanak

POLONIUM

Black Basta

Backdoor Diplomacy

Tropic Trooper

Lazarus

Lapsus$

Fox Kitten

FIN7

Andariel

Karakurt

REvil

admin@338

Luna Moth

(«Silent Ransom Group»)

Morpho

DarkSide

The Shadow Brokers

APT-C-36

Cobalt Group

Anonymous

Ember Bear

NoName057

Deep Panda

Network Crack Program

Wizard Spider

Axiom

LockBit

Lizard Squad

LulzSec

Guardians of Peace

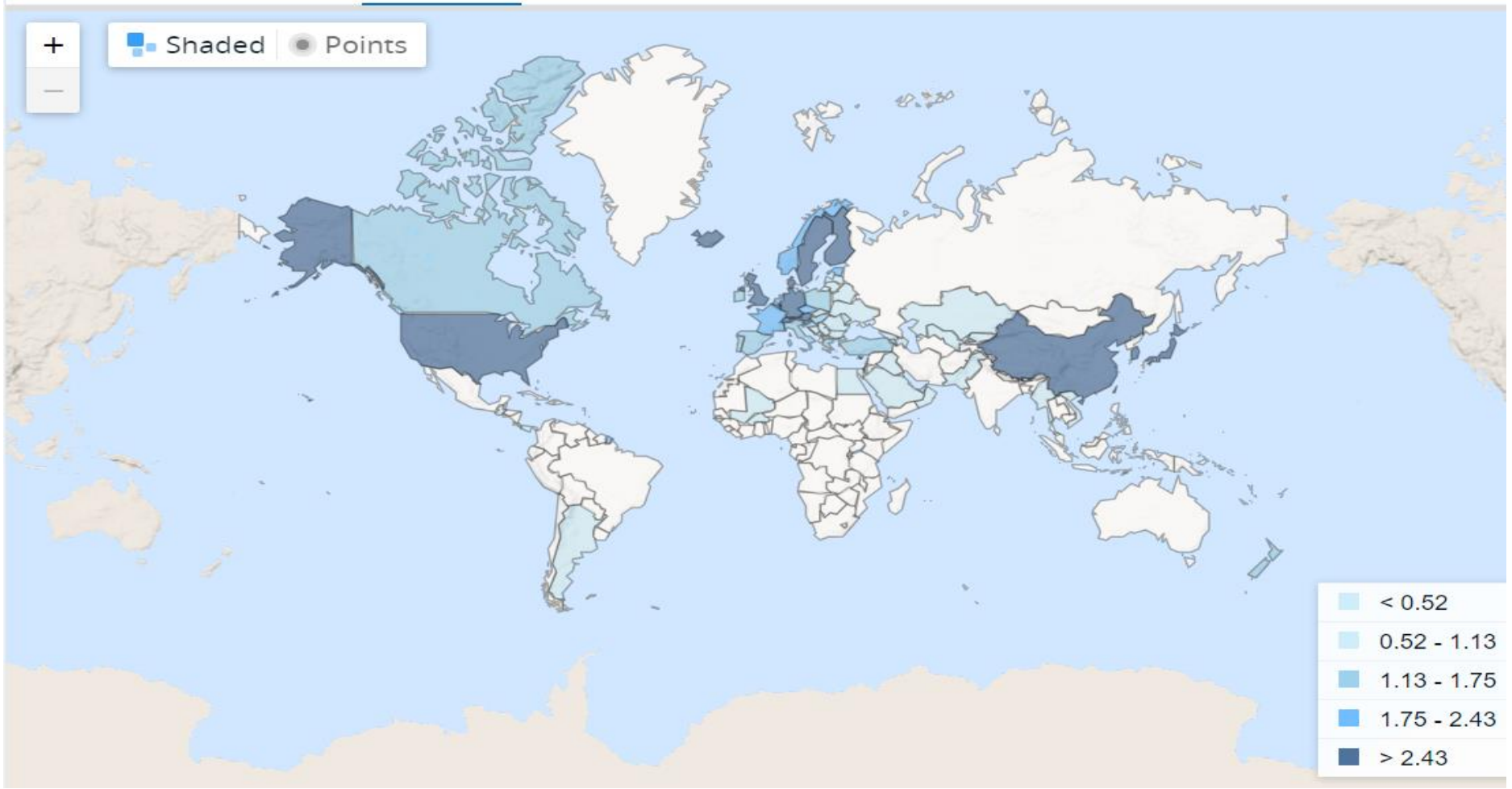
GhostShell

UGNazi

Gasto en investigación y desarrollo (% del PIB)

Instituto de Estadística de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO).

Línea Columna Mapa Compartir Detalles



Correlación entre % gasto de investigación y desarrollo con respecto a la cobertura de Internet

Coeficiente de correlación
0.60074195

Fuente y elaboración propia

¿Qué abarca la ciberseguridad?

(según IBM).

Seguridad de infraestructura fundamental	Seguridad de la red	Seguridad de la aplicación	Seguridad en la nube	Seguridad de información	Recuperación de desastres
Prácticas para proteger la infraestructura física que sostiene materialmente los sistemas informáticos, para la seguridad nacional, la economía y/o la seguridad ciudadana.	Medidas de seguridad para proteger una red informática de intrusos, incluidas tanto las conexiones por cable como inalámbricas (Wi-Fi).	Procesos que ayudan a proteger las aplicaciones que operan en entornos locales y en la nube. La seguridad debe integrarse en las aplicaciones en la etapa de diseño, teniendo en cuenta cómo se gestionan los datos, la autenticación del usuario, etc.	Computación verdaderamente confidencial que cifra los datos en la nube en reposo (almacenados), en movimiento (mientras migran hacia, desde y dentro de la nube) y en uso (durante el procesamiento)	Medidas de protección de datos, que protegen sus datos más confidenciales contra el acceso no autorizado, la exposición o el robo.	Herramientas y procedimientos para responder a eventos no planificados, como desastres naturales, cortes de energía o incidentes de ciberseguridad, con una interrupción mínima de las operaciones principales.

Fuente: IBM (s.f). Elaboración propia.

Global Cybersecurity Index.

International Telecommunication Union.

Cinco pilares

- Medidas legales (L).

- Herramientas técnicas (T) para defenderse de los ciberataques, incluidos los equipos de respuesta.

- Aspectos organizativos (O), es decir, instituciones nacionales para garantizar la ciberseguridad.

- Marco de creación de capacidad (CB) para la certificación; acreditación a nivel nacional (tomansdo como pilar el que está más relacionado con las actividades científicas).

- Cooperación (CP): “abordar el cibercrimen requiere enfoques de múltiples partes interesadas”.

{L, T, O, CB, CP}

National Cyber Power Index

Belfer Center for Science and International Affairs, Harvard Kennedy School

El poder cibernético es el despliegue efectivo de capacidades cibernéticas, por parte de un Estado, para contribuir en el logro sus objetivos nacionales.

$$\text{Índice de ciberpoder nacional} \sum_{x=1}^{8} \text{Capacidad } x * \text{Intención } x$$

National Cyber Power Index.

Belfer Center for Science and International Affairs, Harvard Kennedy School

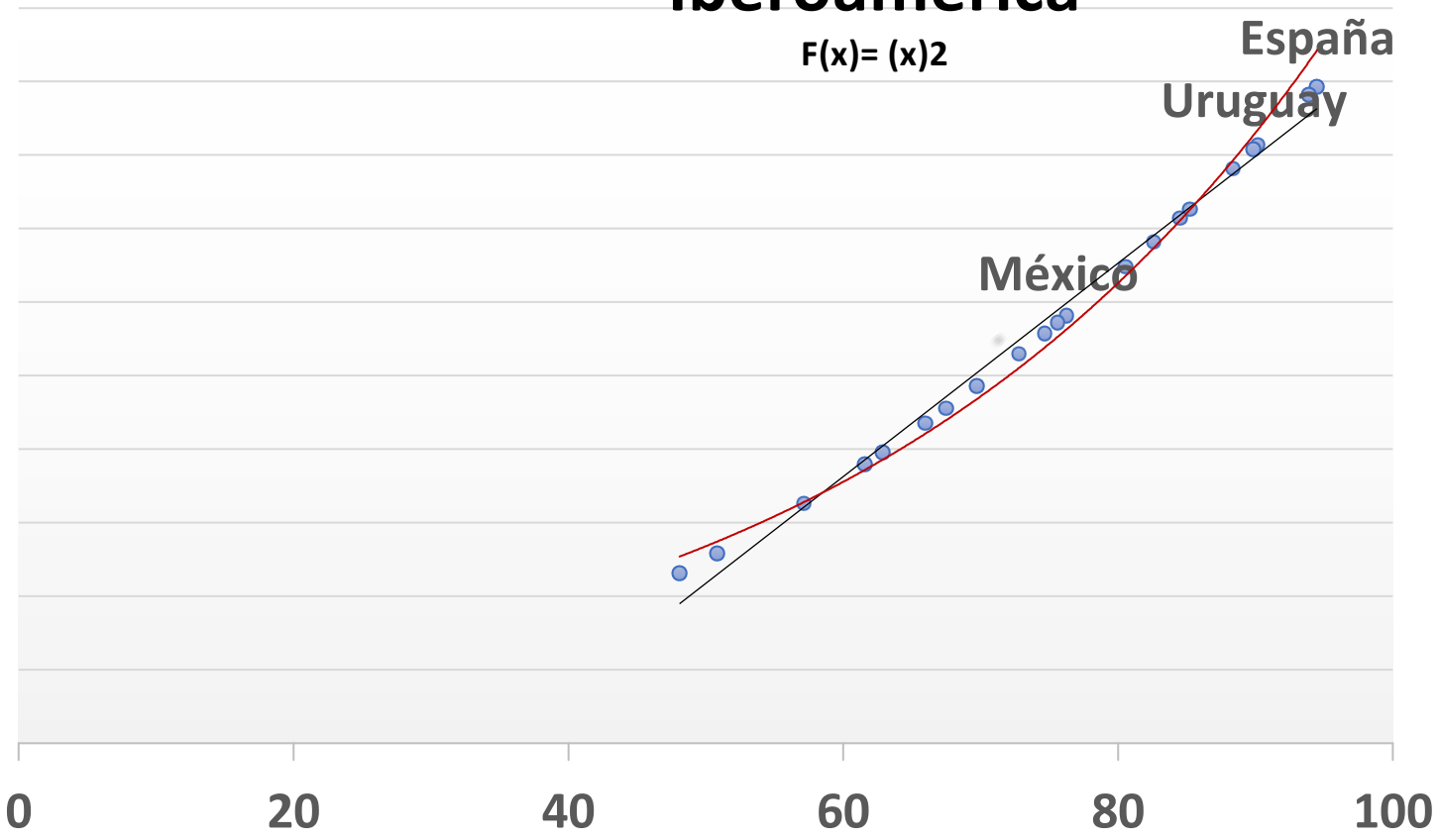
El poder cibernético más completo es el país que tiene:
1) la intención de perseguir múltiples objetivos nacionales utilizando medios cibernéticos y;
(2) las capacidades para lograr esos objetivos.

$$\text{Índice de ciberpoder nacional} \sum_{x=1}^{8} \text{Capacidad } x * \text{Intención } x$$

Para medir el poder cibernético de un país, debemos responder las siguientes preguntas:
1. ¿Qué objetivo(s) pretende perseguir un país en el ciberespacio desde las perspectivas defensivas y ofensivas?
2. ¿Qué capacidades tiene un país para alcanzar esos objetivos?

Objetivos del poder cibernético Los objetivos comunes que los Estados intentarán alcanzar a través del ciberespacio	
Acumulación de Poder y riqueza	Un Estado ha llevado a cabo operaciones cibernéticas para acumular riqueza.
Vigilancia y seguimiento de grupos locales o nacionales	Un Estado ha tomado medidas para monitorear, detectar y recopilar inteligencia sobre amenazas y actores internos dentro de sus propias fronteras. Esto puede abarcar desde esfuerzos para vigilar y monitorear el tráfico de Internet, eludir el cifrado o detectar e interrumpir servicios de inteligencia extranjeros, organizaciones criminales y grupos terroristas.
Fortalecimiento y mejora de las ciberdefensas nacionales	Un Estado ha priorizado la mejora de la defensa de los activos y sistemas gubernamentales y nacionales, así como la resiliencia nacional. Esto incluye la defensa de los activos gubernamentales, la promoción de la ciberseguridad entre las industrias clave y la población en general, y la sensibilización sobre las ciberamenazas.
Controlar el entorno de información.	Difusión de propaganda interna, eliminar material extremista de las redes sociales y refutar la propaganda extranjera.
Recolección de inteligencia extranjera para la seguridad nacional	Recopilación de información que no es comercialmente sensible, vinculada a actividades diplomáticas, planificación militar, seguimiento de tratados y otras situaciones en qué los Estados buscan mejorar su conciencia situacional y su comprensión del extranjero.
Creciente competencia en tecnología cibernética y comercial	Un Estado ha intentado hacer crecer su industria tecnológica nacional o ha utilizado medios cibernéticos para desarrollar otras industrias a nivel nacional. Los medios incluyen inversión en investigación y desarrollo de ciberseguridad y priorizar el desarrollo de la fuerza laboral en ciberseguridad.
Destruir o inhabilitar la infraestructura y las capacidades de un adversario	Un Estado ha utilizado técnicas, tácticas y procedimientos cibernéticos destructivos para disuadir, erosionar o degradar la capacidad de un adversario de luchar en forma cibernética o convencional.
Definición de normas y estándares técnicos internacionales	Un Estado ha participado activamente en debates legales, políticos y técnicos internacionales en torno a las normas cibernéticas.

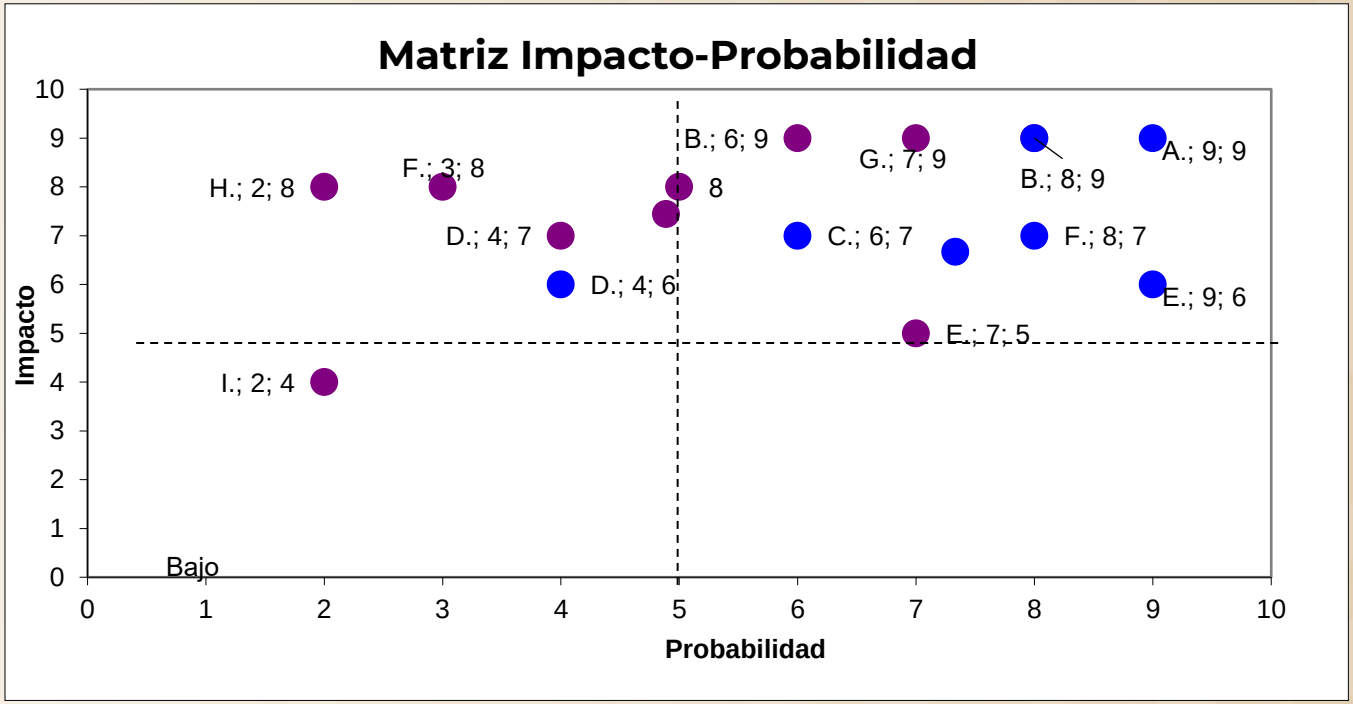
Brecha de cobertura de internet en Iberoamérica



Fuente y elaboración propia

Oportunidades-Amenazas.

Oportunidades	Probabilidad	Impacto
A. Ampliar redes de vigilancia de seguridad nacional	8	9
B. Construcción de estructuras virtuales del desarrollo nacional	6	9
C. Reducción de costos en gastos de seguridad y defensa	5	8
D. Ciberespacio como eje del desarrollo social y de políticas en seguridad	4	7
E. Industria del ciberespacio est´ en desarrollo temprano	7	5
F. Ahorros en desarrollo e investigación	3	8
G. Construcción de bloque regional de ciberdefensa	7	9
H. Creación de tecnología propia	2	8
I. Reducción de grupos cibercriminales en la región	2	4



Amenazas	Probabilidad	Impacto
A. Parálisis de la infraestructura crítica (material)	9	9
B. Ciberdelitos de fuero común y federal en aumento	8	5
C. Ataques a empresas y gobiernos patrocinados por Estados beligerantes	6	7
D. Ausencia de personal especializado ante amenazas cibernéticas	4	6
E. Ataques a infraestructura crítica de información	9	6
F. Robo de información	8	7

Fuente y elaboración propia

Conclusiones.

La sistematización de instrumentos para garantizar la seguridad nacional desde el ciberespacio es una prioridad apremiante para asegurar la paz, la estabilidad y desarrollo de una nación, esto consecuentemente a que el terrorismo, la delincuencia organizada; los grupos extremistas; los Estados beligerantes; hackers, entre otras amenazas, pretenden adueñarse del ciberespacio y a partir de ahí apropiarse del mundo físico que lo sostiene; pero también, esta *nueva frontera* es propicia para aumentar las capacidades del Estado para fomentar la prosperidad colectiva y el combate eficaz en contra de los que se oponen a los objetivos estratégicos que un pueblo se ha determinado alcanzar de manera legítima y legalmente.

Muchas Gracias

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

2024 Felipe Carrillo PUERTO

Referencias.

- Banco Mundial. (2024). Gasto en investigación y desarrollo (% del PIB). Banco Mundial: https://datos.bancomundial.org/indicator/GB.XPD.RSDV.GD.ZS?type=shaded&view=map
- Gibson, W. (1984) Neuromante. Titivillus [versión digital de 2019].
- Gutiérrez, N. (2022). 30 Estadísticas importantes de seguridad Informática. Prey proyect. https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica
- IBM. (s.f). ¿Qué es la ciberseguridad? IBM. https://www.ibm.com/mx-es/topics/cybersecurity
- Imperva (2023). Cyber Warfare. Imperva-a Thales Company. https://www.imperva.com/learn/application-security/cyber-warfare/
- ITU. (2022). The Global Cybersecurity Index. New York: International Telecommunication Union. https://www.itu.int/en/about/Pages/default.aspx
- O'Brien, C. (2021). What is cyber-terrorism, and is it a threat to U.S. national security? Small Wars Journal. https://smallwarsjournal.com/jrnl/art/what-cyber-terrorism-and-it-threat-us-national-security
- Rainer Bruggemann; Peter Koppatz; Margit Scholl; Regina Schuktomow; (2021). Global Cybersecurity Index (GCI) and the Role of its 5 Pillars . Social Indicators Research, (), –. doi:10.1007/s11205-021-02739-y
- Santana-Soriano, E.; Báez, K. (2022). Ciberespacio y cibermundo: delimitaciones conceptuales desde el materialismo sistémico. Ciencia y Sociedad, (47)1: 45-57. https://doi.org/10.22206/cys.2022.v47i1.
- SEDENA-MARINA. (2021). Glosario de Términos SEDENA MARINA en Materia de Seguridad en el Ciberespacio. México: Gobierno de México. https://www.gob.mx/semar/documentos/glorario-de-terminos-de-ciberseguridad?state=published
- TrendMicro-Ponemon. (2023). Cyber Risk Index. Ponemon Institute. https://www.trendmicro.com/es_mx/security-intelligence/breaking-news/cyber-risk-index.html
- Unit 42.(2023). Informe sobre ransomware y extorsión (2023). Ámsterdam: Palo Alto Networks.
- Voo, J., Hemani, I., y Cassidy, D. (2022). National Cyber Power 2022. Cambridge: Belfer Center for Science and International Affairs Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf
- World Economics. (2024). Americas. World Economics. https://www.worldeconomics.com/Regions/Americas/
- World Statistics Pocketbook 2023. https://unstats.un.org/unsd/publications/pocketbook/files/world-stats-pocketbook-2023.pdf
- Zdzikot. T. (2022). Cyberspace and Cybersecurity, en K. Chałubińska-Jentkiewicz et al. (eds.), Cybersecurity in Poland. Varsovia: Warsaw Bar Association. https://www.academia.edu/73195094/Cyberspace_and_Cybersecurity

SEDENA
SECRETARÍA DE LA DEFENSA NACIONAL

2024 Felipe Carrillo Puerto