Vol 4. Nº 3
septiembre - diciembre 2019

Hacia una organización disruptiva en materia de ciberseguridad de la República Bolivariana de Venezuela

Kenny Díaz
Instituto de Altos Estudios para la Seguridad de la Nación (IAESEN)
kennydiazjercito@gmail.com
Venezuela

Carlos Zavarce
Observatorio Nacional de Ciencia Tecnología e Innovación (ONCTI)
ucvpca@yahoo.com
Venezuela

Fecha de recepción: 12/11/2019 - Fecha de aceptación: 05/12/2019

Resumen

Este artículo tiene como objetivo analizar las implicaciones de una organización disruptiva en materia de ciberseguridad de la República Bolivariana de Venezuela. Es un estudio de enfoque documental Se ubica en la discusión e implicaciones que tiene el ciberespacio como objeto de estudio más aún en una organización de carácter militar por cuanto éste se ha constituido como el nuevo campo de batalla por excelencia para materializar la gran estrategia del siglo XXI anunciada por Estados Unidos en la década pasada, que supone doblegar al enemigo con el menor costo, el menor tiempo y con el menor número de bajas posibles. Con esta consigna, surgen nuevas amenazas asociadas al ciberespacio, un nuevo campo de batalla, sin fronteras y asimétrico, que demanda de los estados naciones no importando su tamaño ni ideología, contar con una organización y estrategia nacional altamente adaptativa en materia de ciberseguridad. Se plantea como ideas conclusivas la necesidad de contar con una organización rectora del diseño e implementación de las estrategias de carácter defensivo y ofensivo en materia de ciberseguridad ante la atomización e incapacidad de adaptación del ecosistema organizacional dedicado a detectar, neutralizar y recuperar la operatividad de las infraestructuras críticas del Estado venezolano ante los riesgos latentes en el ciberespacio.

Palabras clave: seguridad; ciberespacio; ciberseguridad; infraestructura crítica; Comando Cibernético Nacional.

Depósito legal: PP201302DC4376 / ISSN: 2343-5984

Towards a disruptive cybersecurity organization in the Bolivarian Republic of Venezuela

Abstract

This article presents the advances of a study that aims to analyze the implications of a disruptive cybersecurity organization in the Bolivarian Republic of Venezuela. It is a multi-method, descriptive field study for which it was necessary to review materials and documents regarding the object to be studied. In an increasingly globalized context, a new area called cyberspace emerges. This area has become the new battleground par excellence to materialize the great strategies of the 21st century announced by the United States in the past decade, which involve defeating the enemy at the lowest possible cost, in the shortest possible time and with the least number of potential casualties. Bearing this slogan in mind, new threats associated with cyberspace arise. It is a new borderless and asymmetrical battlefield that demands that nation-states, regardless of their size or ideology, need to have a highly adaptive national cybersecurity organization and strategy. The concluding ideas show that there is a need for a leading organization to design and implement defensive and offensive cybersecurity strategies. This need arises due to the atomization of the organizational ecosystem that is dedicated to detecting, neutralizing, and recovering the operability of the Venezuelan State's critical infrastructure when faced by latent risks in cyberspace, as well as its inability to adapt to these.

Key Words: Security; cyberspace; cybersecurity; critical infrastructure; National Cyber Command.

Depósito legal: PP201302DC4376 / ISSN: 2343-5984

Vol 4. Nº 3
septiembre - diciembre 2019

Introducción

Probablemente prepararse para la guerra, ha sido, es y seguirá siendo una de las necesidades del ser humano, razón por la cual la organización de la seguridad nacional es sin duda uno de los procesos organizacionales más antiguos del mundo.

De esta manera, en la organización de la seguridad nacional, se han ido incorporando a lo largo del tiempo una cadena de oficios. Al principio únicamente existían lo que identificaremos hoy como combatientes, es decir, los hombres que se encargaban de defender la soberanía de un país y su integridad territorial, para lo cual contaban con el monopolio de las armas y la posibilidad de hacer uso de la fuerza en circunstancias excepcionales. Más adelante en la historia, en algunas naciones aparece los intermediarios o contratistas que no sólo realizan las actividades de comercialización e intermediación de bienes y servicios para el funcionamiento de la seguridad nacional de un país, si no que le son contratadas inclusive operaciones de seguridad nacional.

Ya en tiempos modernos aparecen nuevos oficios asociados a la seguridad nacional como pueden ser los ingenieriles y/o científicos tecnológicos, que, entre otros procesos organizacionales asociados a los diferentes usos de las nuevas tecnologías, se encuentran la prevención, detección y gestión de los incidentes telemáticos generados en los sistemas de información de las plataformas o infraestructuras críticas de una Nación. Esta diversidad de oficios da una idea de la complejidad de la organización de ciberseguridad de una nación, en donde intervienen diversidad de actores y empresas que constituyen este particular ámbito de la seguridad de una nación.

Ahora bien, en la Venezuela de hoy, se están consolidando importantes cambios en todos los aspectos doctrinarios, en concordancia con los lineamientos estratégicos establecidos en el Plan Socialista de Desarrollo Económico y social de la Nación 2019-2025 (Plan de la Patria 2025), y en este contexto, las interacciones entre los actores, se desarrollan con extremada rapidez e imprecisión, obligando a que las decisiones que se deben tomar en la organización de asuntos relacionados con la ciberseguridad, en los diferentes niveles de recursión del Estado, se gesten casi en tiempo real y en coordinación con actores que con frecuencia están alejados de los lugares donde se materializan las ciberamenzas a infraestructuras críticas del Estado Venezolano. Para ello, los decisores requieren de “Conocimiento” e “Informaciones” adicionales que por lo general se producen en los lugares distantes, conocidos como teatros de operaciones, donde se requiere garantizar la adaptación, regulación y control requerida una vez detectada o materializada la ciberamenaza para restablecer el estado de operatividad y retorno a la calma.

Lo anterior, plantea a las instituciones revisar permanentemente sus estrategias en materia de ciberseguridad, para incorporar modelos organizacionales, ante nuevas amenazas que se materializan con incidentes telemáticos que afectan los sistemas de información y plataformas, e infraestructuras críticas, las cuales demandan innovaciones disruptivas en materia organizacional para potenciar la prevención y protección contra ataques, así como la capacidad de respuesta ante los mismos, fortaleciendo la necesaria adaptación que esta particular actividad exige.

Experiencias exitosas de empleo de modelos de organización en ciberseguridad en países aliados (China, Rusia, Irán), indican que es necesario fomentar la necesaria sinergia entre el ecosistema de organizaciones públicas y privadas que haciendo vida en el territorio nacional, tienen las competencias e infraestructuras requeridas para que en materia de ciberseguridad, darle cumplimiento al mandato constitucional relacionado con la seguridad y defensa de la nación, en el emergente ámbito del Ciberespacio.

El tránsito hacia un modelo de organizaciones disruptiva en materia de ciberseguridad facilitaría la obtención de inteligencia, promovería la reducción de costes y horizontalidad entre los actores, simplificando e incrementando la productividad de los procesos organizacionales que garanticen, en la medida de lo posible, el aseguramiento de las redes y sistemas que constituyen el ciberespacio, por medio de la detección y neutralización

Depósito legal: PP201302DC4376 / ISSN: 2343-5984

de intrusos, reacción y recuperación ante incidentes, y preservación de la confidencialidad, disponibilidad e integridad de la información existente en infraestructuras críticas del Estado, para así para afrontar de modo coherente los retos que plantea la utilización del ciberespacio, en una nación que hoy se encuentra asechada por intereses imperiales y que sin duda traen consigo riesgos para la seguridad integral de la nación.

De allí que este artículo se inscribe en esa dirección, para lo cual tomando como eje de comprensión la institucionalidad del estado venezolano para hacerle frente a este tipo de amenazas (organismos dedicados a la ciberseguridad), se reportan los avances de un proceso investigativo en curso, que intenta develar la necesidad de contar con un Comando Cibernético Nacional que garantice la direccionalidad estratégica para detectar a tiempo y/o neutralizar amenazas propias del ciberespacio y que a la vez este alineado con las directrices emanadas en el Plan Socialista de Desarrollo Económico y Social de la Nación 2019-2025 (Op.cit)

Este artículo se estructuró así: a) la introducción; b) Contextualización, donde se aborda una aproximación al fenómeno de Ciberseguridad en Venezuela; c) Acercamiento conceptual; d) Abordaje metodológico; e) Hallazgos iniciales; f) Ideas conclusivas. Finalmente, se presentan las referencias bibliográficas para el desarrollo de éste artículo.

Contextualización

La República Bolivariana de Venezuela no ha permanecido inmune a las agresiones que utilizan el ciberespacio para atentar contra los más variados aspectos de su seguridad nacional, llegando a verse comprometidos servicios críticos como el funcionamiento de Industria Petrolera Nacional en el año 2009, los servicios de pago electrónico en el año 2014, la conectividad prestada por la empresa de Telecomunicaciones del Estado Venezolano Movilnet en el año 2016, las redes sociales y páginas web de instituciones públicas durante los años 2016 al 2018 y durante el año 2019 el intento de magnicidio frustrado contra el Presidente Constitucional de la República Bolivariana de Venezuela, mediante el empleo de tres vehículos aéreos no tripulados de pequeño tamaño (Drones) con cargas de C4, así como el sabotaje al Sistema Eléctrico Nacional; eventos de carácter socio-tecnológicos que sin duda han causado daños irreparables a la seguridad de la nación.

A partir de este último evento, en asocio con especialistas de naciones aliadas como Rusia, China e Irán, se han estudiado en profundidad cuáles fueron las amenazas y los riesgos derivados en materia de Ciberseguridad que los organismos responsables no habían identificado en una estrategia nacional de ciberseguridad.
Estos elementos son en los actuales momentos la base de partida para organizar la cooperación con estas entidades supranacionales en la esfera de la ciberseguridad, la cual ha sido de gran utilidad para identificar nuevas amenazas y riesgos, que aún después del desbastador ataque al Sistema Eléctrico Nacional siguen latentes.

Además, la colaboración con otros actores nacionales como la Fuerza Armada Nacional Bolivariana, el Consejo Científico Tecnológico Nacional, la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), el Cuerpo de Investigaciones, Científicas, Penales y Criminalísticas (CICPC), entre otros, se intenta adecuar la dimensión organizativa del problema e intercambiar experiencias que pudieran eventualmente redundar en un incremento de los niveles en materia de ciberseguridad a nivel nacional.

Todo ello en la aspiración de poder afrontar de modo coherente los retos que plantea la utilización del ciberespacio, en una nación que hoy se encuentra asechada por intereses imperiales que sin duda traen consigo riesgos para la seguridad integral de la nación.

Importa destacar que, ante los eventos reseñados, la institucionalidad del estado venezolano para hacerle frente a este tipo de amenazas (organismos dedicados a la ciberseguridad), se mostró incapaz de anticiparse a estas amenazas, de manera de generar señales de alerta temprana, y mucho

Depósito legal: PP201302DC4376 / ISSN: 2343-5984

Vol 4. Nº 3
septiembre - diciembre 2019

menos estabilizar (lograr adaptación) las infraestructuras afectadas con un tiempo de reacción que fuera imperceptible a los usuarios de las mismas.

Lo anterior, obedeció entre otras causas no sólo a la falta de planes sino a la inexistencia de una organización rectora capaz mantener alineación estratégica de forma de sincronizar las capacidades instaladas en organismos tales como el Comando Estratégico Operacional de la Fuerza Armada Nacional Bolivariana, a través de la Dirección Conjunta de Ciberdefensa (DICOCIBER), el Ministerio de poder popular para la Ciencia y Tecnología a través de sus órganos adscritos como lo son el Centro Nacional de Tecnologías de Información (CNTI), la Super Intendencia de Certificación Electrónica (SUSCERTE), con su Sistema Nacional de Gestión de Incidentes Telemáticos de Venezuela (VenCERT) y el Centro Nacional de Informática Forense (CENIF), que además incorpora al Ministerio del Poder Popular para las Relaciones Interiores, Justicia y Paz a través de la División Contra Delitos Informáticos del CICPC, para ejecutar con calidad estrategias de mitigación de riesgos.

En consecuencia, se evidenciaron vacíos estratégicos y organizacionales para que las capacidades y talentos se alineen en torno al logro de los propósitos que el Estado Venezolano tenga en materia de ciberseguridad, de forma de combatir con calidad las amenazas reales que se ciernen sobre el estado venezolano en esta materia.

Lo anterior, tomando en cuenta las limitaciones existentes desde esta plataforma organizacional, es que se plantea una innovación organizacional en materia de ciberseguridad de la República Bolivariana de Venezuela. De allí la creación del Comando Cibernético Nacional, inspirado en los planteamientos de la Cibernética Organizacional, para fomentar la necesaria sinergia entre el ecosistema de organizaciones públicas y privadas que, haciendo vida en el territorio nacional, tienen las competencias e infraestructuras requeridas para que, en materia de ciberseguridad, darle cumplimiento del mandato constitucional relacionado con la seguridad y defensa de la nación.

Acercamiento conceptual

Ciberespacio y ciberseguridad ambos conceptos son de uso generalizado por parte de amplios sectores de nuestra sociedad. La primera referencia obligada al abordar el tema del ciberespacio es que este es un ámbito relativamente nuevo de actuación y de evolución dinámica, que surge como una nueva dimensión donde pueden materializarse nuevas e insospechadas amenazas. De esta forma si en el pasado estaba claro que geográficamente nos movíamos en las cuatro dimensiones, tierra, mar, aire y el espacio, ahora contamos con una dimensión adicional, y más intangible que las anteriores.

El ciberespacio ha sido definido por Sánchez (2019, p. 20) como

> …un ámbito caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de los sistemas en red y la infraestructura física asociada. El ciberespacio se puede considerar como la interconexión de los seres humanos a través de los ordenadores y las telecomunicaciones, sin tener en cuenta la dimensión física.

No obstante, el empleo de conceptos como ciberdelincuencia o ciberterrorismo son utilizados ampliamente para definir, en el primer caso la "delincuencia vía internet" o en el segundo el "terrorismo a través de la red", han generado en el imaginario de la población la asociación del ciberespacio con el Internet, es decir con el espacio intangible o la nube a la que desde dispositivos electrónicos tenemos acceso a nivel global.

Al respecto, Umphress, (2007) indica que actores (tanto estatales como no estatales) que decidan operar en el ciberespacio, obtendrán una serie de ventajas asimétricas, como son las siguientes: a) El ciberespacio es un "campo de batalla" de grandes dimensiones y donde resulta relativamente fácil asegurar el anonimato. Los ataques se pueden lanzar desde casi cualquier parte del mundo; b) Los efectos de los ataques son desproporcionados con respecto a su coste. Las operaciones se pueden realizar sin necesidad de efectuar fuertes inversiones en recursos humanos y materiales; c) La naturaleza de los ciberataques fuerza

Depósito legal: PP201302DC4376 / ISSN: 2343-5984

a la mayoría de las víctimas, tanto reales como potenciales, a adoptar una actitud defensiva; d) Esta amenaza tiene un alcance global, en la cual el actor (ya sea ciberdelincuente, ciberterrorista, etc.), puede operar desde cualquier parte del mundo con el único requisito de tener acceso al ciberespacio. La conexión al ciberespacio de cualquier sistema lo convierte en un objetivo susceptible de ser atacado; e) Proporciona las herramientas necesarias para que los más pequeños puedan enfrentarse, incluso vencer y mostrarse superiores a los más grandes, con unos riesgos mínimos para ellos.

En consecuencia, estamos en presencia de un nuevo campo de batalla en materia de seguridad como lo es ciberespacio, donde se producen eventos cada vez más insospechados mediante el empleo de sofisticadas técnicas por parte de activistas y delincuentes.

Otro concepto importante para efecto de éste trabajo, es el de la ciberseguridad, al respecto Levin, Goodrick, y Ilkina, (2013) la conceptualizan como "una propiedad del ciberespacio, que tiene la capacidad de resistir las amenazas intencionales y no intencionales, responder y recuperarse" (p.8)

En el trabajo de. Rain, y Peeter. (2010), se recoge el estado actual de debate existente sobre este objeto de estudio al indicar que, sobre la materia, planteando que:

> …el conjunto de actuaciones orientadas a asegurar, en la medida de lo posible, las redes y sistemas que constituyen el ciberespacio detectando y enfrentándose a intrusiones, - detectando, reaccionando y recuperándose de incidentes, y -preservando la confidencialidad, disponibilidad e integridad de la información (s/p)

Esta definición permite situar los ciberataques en perspectiva con otros riesgos globales; y en tal sentido, el estudio de Riesgos Globales (2019) producto del Foro Económico Mundial del año 2019 ofrece en la figura Nº 1 la percepción del impacto y de la probabilidad de los riesgos globales, que denomina el paisaje de riesgos globales en 2019.

En dicho Foro se debatió que asistimos a un momento en que las oportunidades de las tecnologías emergentes exigen audacia y agilidad, un aumento en los ataques cibernéticos afiliados al estado está agravando los puntos de falla en las operaciones de la empresa, la infraestructura, las cadenas de suministro y las interacciones con los clientes.

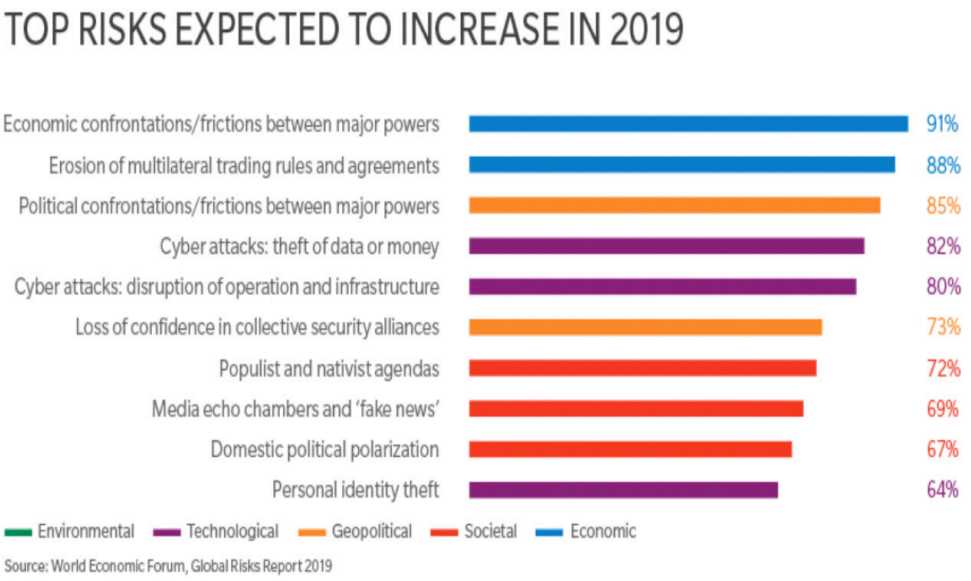

Figura Nº 1. Panorama Global de Riesgos en el 2019
Fuente: Fondo Económico Mundial (2019)

Depósito legal: PP201302DC4376 / ISSN: 2343-5984

Vol 4. Nº 3
septiembre - diciembre 2019

La figura Nº 1 permite apreciar que la tecnología sigue desempeñando una función fundamental en la configuración del panorama global de riesgos, y que las preocupaciones sobre el fraude de datos y los ataques cibernéticos volvieron a ser prominentes; también pone de relieve otras vulnerabilidades tecnológicas: alrededor de dos tercios de los encuestados esperan que los riesgos asociados con las noticias falsas y el robo de identidad aumenten en 2019, mientras que tres quintas partes perciben lo mismo sobre la pérdida de la privacidad de las sociedades y los gobiernos.

En 2018, se produjeron nuevas filtraciones masivas de datos, se revelaron nuevas debilidades de hardware y la investigación señaló los usos potenciales de la inteligencia artificial para diseñar ciberataques más potentes. Durante el año 2018 también se demostró que los ciberataques plantean riesgos para las infraestructuras críticas, lo que llevó a los países a reforzar el control de las asociaciones transfronterizas por motivos de seguridad nacional.

De igual manera, en el estudio de Riesgos Globales 2019 (Opcit) reporta que el inicio del año 2019, los ciberataques tienen asignada una probabilidad de 5,1 y un impacto de 4,9. Los riesgos asociados a los ciberataques son superados solamente, en relación a la combinación de ambos parámetros, por el desempleo, la negativa adaptación al cambio climático, las crisis relacionadas con el agua y los conflictos entre Estados. De este paisaje de riesgos globales se desprende la percepción de la alta probabilidad y el elevado impacto de los ciberataques en comparación con el resto de riesgos globales.

De igual forma, en el documento antes indicado, se recoge que el riesgo de ataques cibernéticos a gran escala se sigue considerado por encima del promedio en las dos dimensiones del impacto y la probabilidad, lo que refleja la creciente sofisticación de los ataques cibernéticos y el surgimiento de la hiperconectividad, con un número cada vez mayor de objetos físicos conectados a Internet, además de la vulnerabilidad que supone el almacenamiento de los datos personales en la nube. Además, el "Internet de las cosas" (IoT en sus siglas en inglés) incrementará esta tendencia.

En esta dirección, el mencionado informe resalta la conexión directa de los ciberataques con otros riesgos tecnológicos como la ruptura de la infraestructura de información crítica, el mal uso de las tecnologías, el fraude y robo de datos. También indica que existe un enlace directo con un riesgo que en el informe se asocia a la economía, el fallo de infraestructuras críticas.

El resto de conexiones directas con otros riesgos caen en el ámbito de los riesgos denominados geopolíticos, ataques terroristas, fallo de la gobernanza nacional y conflictos entre Estados.

La Disrupción Organizacional

En la actualidad resulta difícil referirse al tema de innovación organizacional sin aludir a estructuras dinámicas y flexibles, centradas en procesos, que viabilicen la adaptación, regulación y control e las actividades de cualquier organización, no importando su tamaño y naturaleza. Por ello, el acercamiento del autor para analizar la disrupción organizacional es a través de la teoría cibernética, reconocida como la ciencia que estudia la adaptación, la regulación, el control y la comunicación en los sistemas de cualquier naturaleza pero que presentan un denominador común: Pueden mostrar un comportamiento de adaptación y de autorregulación.

En general, el término cibernética proviene de las voces griegas "Kubepv-aw", que significa gobernar, conducir, que en latín es guberno, gubernavi, gubernatum, y de Kubepnths, que denota piloto, gobierno y que en latín es, guber. Esta palabra, era usada en la antigua Grecia para formar nombres en las artes y las ciencias, y fue tomado por Norbert Weiner, conjuntamente con el vocablo "kybernet" para denominar la Teoría que formulara y que posteriormente se llamaría "Cybernetics", y en castellano "Cibernética".

Esta teoría se colectiviza a partir de 1948, con la aparición del libro "Cibernetics: On Control and

Depósito legal: PP201302DC4376 / ISSN: 2343-5984

communication in the Animal and the Machine" publicado por Norbert Wiener, convirtiéndose en la génesis de un importante pensamiento que ha desarrollado un enfoque propio que permite abordar y explicar, el comportamiento de fenómenos naturales y sociales. De allí surge una definición de la cibernética como la ciencia del control y la comunicación en el animal y en la máquina.

No obstante, una definición más actualizada del concepto cibernética, la proporciona Beer (1985), quien plantea que:

> La cibernética es la ciencia que estudia la adaptación, la regulación, el control y la comunicación en los sistemas de cualquier naturaleza pero que presentan un denominador común: pueden mostrar un comportamiento de adaptación y de autorregulación. De allí que es definida como la ciencia de la organización eficaz. (p.30)

La cibernética nos provee de una teoría precisa y de carácter universal para el estudiar los procesos de adaptación y control de sistemas de cualquier tipo, tamaño y complejidad. Y por ello la actual tendencia a estudiar, bajo el enfoque cibernético, el funcionamiento de organizaciones, sean estas 'empresariales, gubernamentales o sociales, con el uso intensivo y extensivo del modelo de organización cibernética que permite estructurar organizaciones complejas para el logro de la adaptación, la regulación y el control. Tanto la adaptación como la autorregulación suponen aprendizaje y esto, finalmente, constituye la garantía de sobre vivencia de cualquier sistema.

De este modo, el Modelo de Sistemas Viables (MSV) propicia la representación de la complejidad organizacional sobre la base de la imbricada coexistencia de cinco grandes procesos que se materializan en toda organización: Operativos, Coordinación, Gerencia, Inteligencia y Política; con lo cual se facilita el diagnóstico, análisis y diseño organizacional, en la dirección de garantizar la eficacia y eficiencia necesaria para el fortalecimiento de la capacidad de adaptación, regulación y control organizacional.

Abordaje Metodológico

El trabajo se aborda mediante un enfoque documental apoyado con entrevistas focalizadas. En el primer caso, se utilizó la técnica de análisis de contenido para lo cual se examinaron referencias bibliográficas relacionadas con organizaciones disruptivas, ciberseguridad, cibernética, organización militar de la República Bolivariana de Venezuela. Del análisis se derivaron descriptores cuyos contenidos se discutieron en el abordaje conceptual y que permitieron a los autores contrastar al análisis de los documentos con respecto a lo que opinaron los informantes claves seleccionados para este trabajo. Esto condujo a los autores a analizar, interpretar, relacionar los materiales documentales para avanzar en el camino que conduce hacia una innovación disruptiva en la organización de los asuntos militares vinculado con la ciberseguridad de la República Bolivariana de Venezuela.

Hallazgos

Los hallazgos iniciales indican que la ciberseguridad afecta la seguridad nacional, y en consecuencia impacta los distintos ámbitos que la conforman: ámbito económico, social, político, cultural, geográfico, ambiental y militar. Los desafíos son complejos y satisfacerlos requiere de la voluntad política para impulsar un proceso disruptivo que conduzca al diseño e implementación de organización que revoluciones los asuntos militares relacionados con la seguridad en el ciberespacio de la República Bolivariana de Venezuela.

Además, la cibernética nos provee de una teoría precisa y de carácter universal para el estudiar los procesos de adaptación y control de sistemas de cualquier tipo, tamaño y complejidad. Y por ello la actual tendencia a estudiar, bajo el enfoque cibernético, el funcionamiento de organizaciones, sean estas 'empresariales, gubernamentales o sociales, con el uso intensivo y extensivo del modelo de organización cibernética que permite estructurar organizaciones complejas para el logro de la adaptación, la regulación y el control. Tanto la adaptación como la autorregulación suponen

Depósito legal: PP201302DC4376 / ISSN: 2343-5984

aprendizaje y esto, finalmente, constituye la garantía de sobre vivencia de cualquier sistema.

Los hallazgos obtenidos del análisis documental plantean que desde el año 1998 a la fecha indican la inexistencia de una organización rectora de la estrategia nacional en materia de ciberseguridad; con lo cual se evidencia la vulnerabilidad estratégica que supone este tipo de amenazas comprende especialmente dos campos. Por un lado, los ataques contra los sistemas que regulan infraestructuras básicas para el funcionamiento de un país –como el sabotaje de la plataforma tecnológica que soportan la industria petrolera, la de los servicios públicos como telecomunicaciones, banca, la paralización de la red de transporte ferroviario y de tracción por cable, la interrupción de la energía eléctrica a nivel nacional– que suponen un serio deterioro para la normalidad y la seguridad de la sociedad venezolana.

Por otro lado, la penetración en la red de comunicación, mando y control de las Fuerza Armada Nacional Bolivariana, y el sistema nacional de gestión de crisis o en las bases de datos de los servicios de inteligencia con el propósito de cometer magnicidio empleando sistemas no tripulados (drones) supone sin duda una amenaza directa a la seguridad nacional.

Así mismo, al indagar sobre lo que piensan los actores con respecto a la temática se indicó que indicar que cualquier metodología de gestión de riesgos cibernéticos, pasa porque, en primer lugar, se consideren cuáles son los activos del ciberespacio venezolano, cuyas infraestructuras críticas se agrupan en diez (10) sectores importantes: fuerza armada, energía, telecomunicaciones, banca y finanzas, transporte multimodal, salud, agua, alimentos, tecnologías de la información y las comunicaciones. Todos estos sectores se apoyan con mayor o menor intensidad en el ciberespacio, por tanto, es vital conocer el mapa de ciber amenazas que se ciernen sobre ellos. Y en segundo lugar reconocer que el estado venezolano debe dotarse de una organización que rectorice el diseño de estrategias y la doctrina operacional de ciberseguridad que necesita la República Bolivariana de Venezuela en este entorno único de amenazas para el empleo de las capacidades nacionales, necesarias para impedir cualquier tipo de agresión cibernética que pueda amenazar la seguridad nacional.

En relación al sector empresarial, los informantes coinciden en que favorablemente la mayor parte de las grandes empresas han incorporado la gestión de la seguridad a sus prácticas empresariales. No así, las pequeñas y medianas donde, aunque las tecnologías de información y comunicación han sido incorporadas como un factor crítico de éxito en su actividad, estas no han contemplado un nivel de seguridad acorde debido a la falta de recursos económicos y humanos.

Un hallazgo no menos importante es el que revela la opinión de los informantes consultados, que indica que, en los actuales momentos el estado venezolano está en riesgo de ser incapaz de repeler un ciberataque a menos organice de manera disruptiva las capacidades existentes para soportar una estrategia de ciberseguridad.

En consecuencia, debería centralizarse la gestión de la ciberseguridad con la creación de un organismo responsable de coordinar a todas las entidades públicas y privadas implicadas en la República Bolivariana de Venezuela. Todo ello sin olvidar la cooperación internacional en esta materia y fomentar una cultura de ciberdefensa y una promoción de la I+d+i en el sector de la ciberseguridad.

En este contexto, se propone una organización disruptiva en materia de ciberseguridad de la República Bolivariana de Venezuela, bajo la denominación de Comando Cibernético Nacional, que desde el paradigma Cibernético, explore la posibilidad de repensar su andamiaje organizativo, de forma de poder emular mecanismos de adaptación, regulación y control, que siendo exitosos en los seres vivos, para alcanzar máxima eficacia y eficiencia, puede servir como plataforma conceptual para coadyuvar en la creación de una organización dedicada a la ciberseguridad nacional.

El modelo de organización propuesto estará centrado en

Depósito legal: PP201302DC4376 / ISSN: 2343-5984

procesos decisionales, sustantivos y de apoyo, elementos de conformidad con lo pautado en la Ley Orgánica de la Administración Pública.

Teniendo estas orientaciones como telón de fondo, a continuación, se presenta de una manera esquemática la morfología organizativa para Comando Cibernético Nacional, derivado de los principios de la teoría Cibernética, y que con el auxilio del Modelo de Sistemas Viables (MVS) (Figura Nº 2) .

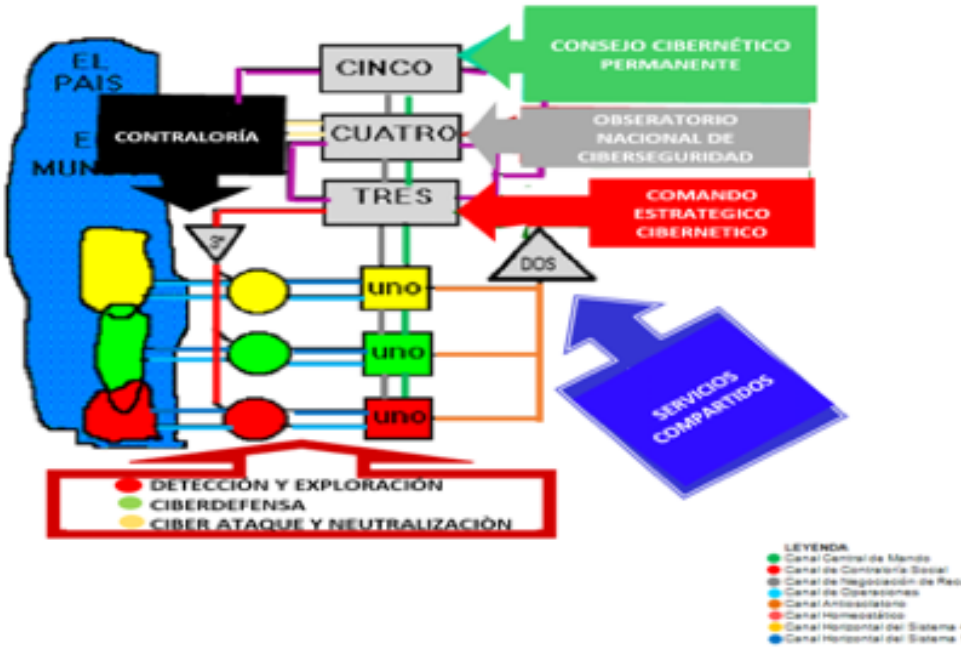

Figura Nº 2. Modelo de Organización Cibernética del Comando Cibernético Nacional para la República Bolivariana de Venezuela.

De allí que, la estructura organizativa del Comando Cibernético Nacional pude concebirse como una estructura organizacional recursiva, constituida por distintos niveles de recursión, que contienen unidades organizacionales que hoy existen y que pasaran a formar parte de esta, que la vez estará contenidas en un sistema mayor. Esta concepción de como estructurar una institución, ofrece la posibilidad de asumir una estructura que apunte hacia la garantía del logro de la necesaria adaptación, regulación y el control de la organización, que permite que quien "Dirige" o quien "Comanda", pueda estar al tanto de lo que está sucediendo en el contexto interno y externo con el cual se interactúa.

Conclusión

Esta particular situación implica que los diseñadores de la estrategia nacional de seguridad y defensa, han de reconocer la existencia de un nuevo ámbito en esta materia, en el que emergen actores, interacciones, procesos y lógicas organizativas, que basan su existencia y formas de acción en principios no tradicionales como la ubicuidad, la convergencia y la molecularización que habita la interconexión en redes de carácter planetarias; aspectos estos que en los actuales momentos han de marcar el debate epistemológico y praxiológico sobre el cómo concebir un Comando Cibernético Nacional, a partir de la reorganización de las diferentes instituciones del estado con competencia en la materia, para contribuir en demasía con la Seguridad, Defensa y Desarrollo Integral de la Nación.

Depósito legal: PP201302DC4376 / ISSN: 2343-5984

Vol 4. Nº 3
septiembre - diciembre 2019

De allí que los diseñadores de la estrategia nacional de seguridad y defensa, se enfrentan ante el reto de la emergencia de nuevas amenazas, que el Estado debe identificar, neutralizar y por sobre todo comprender ante las legítimas preocupaciones sociales de un pueblo que está bajo el asecho de un modelo de guerra multidimensional, multiforme, no convencional que nos demanda eficacia y eficiencia en el manejo de los recursos tecnológicos que el Estado asigna para solventar amenazas cibernéticas que en mayor o menor medida han afectado y afectan a la sociedad venezolana.

Esta inédita situación, plantea la necesidad y oportunidad de repensar mediante el empleo creativo de los postulados de la cibernética, la lógica organizacional que habrá de inspirar el Comando Cibernético Nacional, que por lo demás choca con la lógica de las organizaciones tradicionales que tienen responsabilidad en la materia; lo cual permite explorar una forma innovadora de producción de saberes y comprensión de la dinámica y compleja realidad de la una eventual organización rectora del tema de la ciberseguridad, que habrá de ser pilar de la nueva institucionalidad para la Ciberseguridad de la Nación.

En este contexto, en este artículo invocó los principios que irrumpen de la Cibernética, más concretamente de la Cibernética Organizacional, para como marco referencial para procurar conocer y comprender la complejidad a la que se enfrenta el Estado Venezolano en este emergente ámbito de la Seguridad de la Nación.

Referencias Bibliográficas

Beer, S. (1985). Diagnosting The System for organizations. Gran Bretaña: John Wiley & Sons.

Foro Económico Mundial (2019). Estudio “Riesgos Globales 2019”. En Red. Disponible en: https://es.weforum.org/ [Consulta: 2019, octubre 21].

Levin, A., Goodrick, P., & Ilkina, D. (2013). Securing Cyberspace: A comparative review of strategies worldwide. The 2014 IT Canadian Conference. http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_cyber_crime_final_report.pdf [Consulta: 2019, junio 15].

Losada, R. y Casas, A. (2008). Enfoques para el análisis político. Historia, epistemología y perspectivas de la ciencia política. Bogotá: Pontificia Universidad Javeriana.

Narvarte, P. (2002). Bases teórico-metodológicas para el diagnóstico y diseño de organizaciones. [Transcripción en línea]. Disponible: http://www.comenius.usach.cl/.../DIAGNOSTICO%20Y%20DISEÑO%20ORGANIZACIONAL1.doc. [Consulta: 2019, marzo 21].

Plan Socialista de Desarrollo Económico y social de la Nación 2019-2025. Presidencia de la República Bolivariana de Venezuela. [Transcripción en línea]. Disponible: http://www.gobiernoenlinea.ve.noticias-view/shareFile/PDN.pdf. [Consulta: 2019, Noviembre 10, 12 y 16].

Rain O., & Peeter. L (2010) Cyberspace: definition and implications. Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia.

Sánchez, G. (2019). Ciberguerra y ciberterrorismo ¿realidad o ficción? Una nueva forma de guerra asimétrica. Instituto Universitario General Gutiérrez Mellado, 2019.

Umphress, D. (2007). El Ciberespacio. ¿Un aire y un espacio nuevo?, Air & Space Power Journal. Tercer Trimestre.

Depósito legal: PP201302DC4376 / ISSN: 2343-5984