Revista Latina de Comunicación Social
ISSN 1138-5820 / No. 82, 01-20.
https://doi.org/10.4185/rlcs-2024-2134

Estrategia de comunicaciones de seguridad de la información como requisito previo para contrarrestar la guerra híbrida: experiencia mundial

Information Security Communications Strategy as a Prerequisite to Counteracting Hybrid Warfare: World Experience

Arailym Nussipova
Departamento de la Corporación Educativa Internacional de la Universidad Kazajo-Americana. República de Kazajistán.
arailym_nussipova@sci-academy.cc

Gulzhan Khussainova
Departamento de Disciplinas Sociales y Políticas de la Universidad Regional K. Zhubanov de Aktobe. República de Kazajistán.
gulzhan_khussainova@un-nyc.net

Raushangul Kabilova
Departamento de la Corporación Educativa Internacional de la Universidad Kazajo-Americana. República de Kazajistán.
raushangul_kabilova@sci-academy.cc

Esenzhol Aliyarov
Asociación de Estudios Políticos. República de Kazajistán.
esenzhol_aliyarov@pltch-sci.com

Botakoz Nuralina
Departamento de la Corporación Educativa Internacional de la Universidad Kazajo-Americana. República de Kazajistán.
botakoz_nuralina@sci-academy.cc

Cómo citar este artículo / Referencia normalizada:

Nussipova, A., Khussainova, G., Kabilova, R., Kabilova, R., Aliyarov, E. y Nuralina, B. (2024). Information security communications strategy as a prerequisite to counteracting hybrid warfare: world experience

[Estrategia de comunicaciones de seguridad de la información como requisito previo para contrarrestar la guerra híbrida: experiencia mundial]. *Revista Latina de Comunicación Social*, 82, 01-20.
https://www.doi.org/10.4185/RLCS-2024-2134

Fecha de Recepción: 23/05/2023
Fecha de Aceptación: 18/07/2023
Fecha de Publicación: 21/11/2023

RESUMEN

Introducción: Se destaca la relevancia del estudio ante la necesidad de herramientas innovadoras para contrarrestar amenazas híbridas en el ámbito de la seguridad de la información. **Metodología:** Se describe el enfoque metodológico del estudio, destacando la aplicación de métodos como análisis, sistematización y comparación. Se subraya la utilización de estos métodos para llevar a cabo un análisis comparativo integral de las estrategias de seguridad de la información en Ucrania, Kazajstán y la Unión Europea. **Resultados:** Se enfatiza que los resultados del estudio proporcionan una visión detallada del estado actual de la seguridad de la información en los países analizados. Se menciona específicamente que las recomendaciones para el desarrollo de estrategias de comunicaciones de seguridad de la información son el resultado tangible de la investigación. **Conclusiones:** Se concluye resaltando la importancia de desarrollar o mejorar las estrategias de comunicación de seguridad de la información en los países estudiados. Se sugiere que estas estrategias pueden servir como contramedida efectiva contra la guerra híbrida y ataques enemigos, fortaleciendo la ciberseguridad y la capacidad de respuesta.

Palabras clave: Ciberseguridad; Comunicaciones estratégicas; Seguridad; Información; Guerra híbrida.

ABSTRACT

Introduction: The relevance of the study is underscored in response to the need for innovative tools to counter hybrid threats in the field of information security. **Methodology:** The study's methodological approach is described, highlighting the application of methods such as analysis, systematization, and comparison. The use of these methods is emphasized in conducting a comprehensive comparative analysis of information security strategies in Ukraine, Kazakhstan, and the European Union. **Results:** It is emphasized that the study's results provide a detailed insight into the current state of information security in the analyzed countries. It is specifically mentioned that recommendations for the development of information security communication strategies are a tangible outcome of the research. **Conclusions:** The conclusion highlights the importance of developing or enhancing information security communication strategies in the countries under study. It is suggested that these strategies can serve as an effective countermeasure against hybrid warfare and enemy attacks, thereby strengthening cybersecurity and responsiveness.

Keywords: Cybersecurity; Strategic communications; Security; Information; Hybrid warfare.

1. Introducción

La seguridad de la información está cobrando relevancia en el sistema de seguridad nacional y en el orden mundial en el siglo veintiuno (Sopilko, 2022). El estado que tiene ventaja en la guerra mediática e informativa y en la protección de la información puede liderar en los ámbitos económico, militar-político y otros. Dicho estado también obtiene beneficios estratégicos y tácticos, regula de manera más flexible los costos económicos para el desarrollo de armas y equipos militares, y mantiene la ventaja en numerosas tecnologías avanzadas.

"La seguridad de la información es una característica de un sistema de administración pública estable y sostenible, que mantiene sus componentes vitales cuando se enfrenta a amenazas internas y externa."

La seguridad de la información es una parte integral del desarrollo de la sociedad de la información, lo que implica la expansión de las oportunidades tecnológicas para el intercambio de información (Belkin *et al*., 2022). También significa que todos los sujetos de las relaciones de información (propietarios y usuarios de información, fabricantes de tecnologías y herramientas de información, proveedores de servicios y el estado) son conscientes de la necesidad de implementar todas las medidas para garantizar los recursos de información y la seguridad de la información del estado. Dado que la información tiene una influencia directa en la sociedad, es posible contrarrestar las amenazas de información mediante una interacción efectiva entre el estado y la sociedad civil y una estrategia de comunicación de alta calidad dentro del estado y a nivel internacional.

Las tendencias importantes en la etapa actual del desarrollo humano son la intensificación de los flujos de información transfronterizos y la acumulación de formas y medios de intercambio de información que están prácticamente fuera del control del estado. Nuevas amenazas y desafíos de información son generalizados en este contexto, lo que requiere que los estados respondan de inmediato y tomen medidas y soluciones innovadoras. En este sentido, la seguridad de la información y su estrategia de comunicación se convierten en un tema prioritario en la "agenda" a nivel internacional, regional y nacional.

La seguridad de la información es parte de la seguridad nacional y se define como la protección de la soberanía del estado, la integridad territorial, el orden constitucional democrático y otros intereses nacionales. La ciberseguridad es parte de la seguridad de la información. La seguridad de la información se refiere a la información en general, y la ciberseguridad se centra en la información en sistemas de tecnología de la información. El desarrollo y la implementación de un sistema de medidas de seguridad de la información involucran lo siguiente: determinación del nivel mínimo de funcionalidad de la infraestructura de la información y provisión del nivel de funcionamiento en situaciones de crisis; determinación de contramedidas en caso de emergencia si la infraestructura crítica es atacada; desarrollo de métodos de prueba para herramientas de seguridad; mejora de sistemas para identificar y monitorear interferencias electromagnéticas en la infraestructura crítica; fortalecimiento de la infraestructura de Internet; mejora de la seguridad de los sistemas de control, etc.

En el siglo veintiuno, el mundo enfrenta uno de los principales desafíos, la falta de una estrategia unificada y coordinada para abordar las amenazas a la seguridad global y nacional. Las comunicaciones estratégicas pueden ayudar a enfrentar este desafío. La situación comunicativa actual en el mundo se llama una situación de post verdad. Incluso el Diccionario Oxford de la Lengua Inglesa incluye este concepto y proporciona la siguiente definición: acciones políticas y pensamiento "en los cuales los hechos objetivos tienen menos influencia en la formación de la opinión pública que las apelaciones a las emociones y creencias personales" (Diccionario Oxford de la Lengua Inglesa, 2022). La propaganda, la "intensa actividad", la ideología y la desinformación son conceptos que se pueden atribuir a las herramientas de la guerra de la información, cuyo propósito es la dominación de la información.

El mundo tomó conciencia de la importancia de la comunicación efectiva con todas las partes interesadas solo con la invasión a gran escala de Ucrania por parte de Rusia. La lista de partes interesadas es la siguiente: organizaciones de seguridad internacional y países extranjeros (tanto participantes en el proceso de negociación como fuera de él); organizaciones gubernamentales y ministerios, instituciones de todos los poderes del gobierno; organizaciones no gubernamentales (tanto internacionales como nacionales); autoridades locales; audiencias internas de las instituciones de seguridad. Las comunicaciones estratégicas representan no solo una tendencia en asegurar la seguridad de un país y del mundo globalizado, sino también un desafío. Los expertos de las instituciones de seguridad y gobierno que ocupan diferentes niveles de posición deben aprender cómo implementar estrategias de comunicación, entender la posición del otro y coordinar acciones conjuntas de manera adecuada, contrarrestar influencias destructivas y generar sentimientos positivos (Kordunian, 2022).

La definición principal de comunicaciones estratégicas se propuso en 2010 en el Concepto Militar de Comunicaciones Estratégicas de la OTAN: "Las comunicaciones estratégicas son el uso coordinado y apropiado de las actividades y capacidades de comunicación de la OTAN: Diplomacia Pública (PD), Asuntos Públicos (PA), Asuntos Públicos Militares (PMA), Operaciones de Información (InfoOps) y Operaciones Psicológicas (PsyOps), según corresponda, en apoyo de las políticas, operaciones y actividades de la alianza, y para avanzar en los objetivos de la OTAN. Dentro de la estructura militar de la Alianza, la efectividad de la comunicación estratégica de la OTAN se logrará principalmente a través de las capacidades profesionales de comunicación militar existentes" (Concepto Militar de la OTAN para Comunicaciones Estratégicas, 2010).

La tarea clave de la estrategia de comunicación es proporcionar apoyo informativo para el desarrollo del estado y los negocios. La estrategia de comunicación se basa en la autopresentación y en estrategias creativas y mediáticas. Es un conjunto de herramientas más efectivas para influir en audiencias específicas y un programa particular para utilizar estas herramientas. Los recursos históricos y culturales y la posición del líder regional determinan la efectividad de estrategias particulares en cada sujeto. Ejemplos de estrategias de comunicación efectivas para la seguridad de la información se pueden observar en países que han enfrentado la guerra híbrida, como Estonia y Georgia. Estos países han establecido divisiones y programas especiales para proteger la información y han llevado a cabo campañas para concienciar al público sobre los ciberataques y la desinformación.

Ucrania es un excelente pero triste ejemplo de cómo la falta de uso de las comunicaciones estratégicas en el país ha llevado a una amenaza para la seguridad nacional, desinformación total, agencia de información y guerra híbrida. Desde el inicio de la agresión rusa contra Ucrania en 2014, los representantes del sector de seguridad y defensa y los voluntarios han comprendido que la cuestión de las comunicaciones estratégicas es una herramienta efectiva en el contexto de la guerra de información híbrida llevada a cabo por la Federación Rusa contra Ucrania. La tecnología de StratCom permite al estado ser capaz y resistente para hacer frente a las amenazas de información modernas.

Además, los países desarrollados están intensificando las actividades gubernamentales en la dirección de la regulación legislativa de las relaciones en el espacio de información nacional. Siguiendo este propósito, tales países respaldan regulaciones especiales para la implementación de las bases prioritarias de la política estatal de información. La necesidad de analizar la seguridad de la información y la estrategia de comunicación como un requisito previo para contrarrestar la guerra híbrida ha condicionado este estudio. Las principales fuentes de investigación fueron los actos legales de la Unión Europea, Ucrania y la República de Kazajistán, y otros materiales oficiales, incluyendo comunicados de prensa, datos estadísticos, informes de investigaciones sociológicas, etc. Un estudio comparativo de los mecanismos de Ucrania, Kazajistán y la Unión Europea para garantizar la seguridad de la información implicó el estudio de actos legales reguladores y otras fuentes legales de los estados mencionados, así como materiales de estudios sociológicos en el ámbito del uso de la televisión y el Internet en Ucrania, la República de Kazajistán y la Unión Europea.

La falta de estudios sobre estrategias de comunicación de seguridad de la información en el contexto de un análisis comparativo de la Unión Europea, Ucrania como un país con un firme enfoque en la integración europea, y Kazajistán como uno de los países avanzados de Asia Central, hace que esta investigación sea relevante. El análisis comparativo de las estrategias de seguridad de la información de Ucrania, Kazajistán y la Unión Europea revelará similitudes y diferencias en los enfoques de estos países y el bloque regional para la protección de la información y la lucha contra las amenazas cibernéticas. Los materiales del artículo pueden ser útiles para expertos en política, especialistas en relaciones públicas, expertos en relaciones públicas, desarrolladores de estrategias de comunicación, campañas de información y actos legales reguladores en el ámbito de la seguridad de la información.

2. Revisión de la literatura

Como parte del estudio, los autores analizaron numerosas obras científicas de académicos kazajos, rusos y extranjeros dedicadas a cuestiones de seguridad de la información y sus aspectos, en particular, las guerras de información y el impacto de la información.

Los siguientes investigadores rusos resumieron de manera adecuada cuestiones generales y específicas del desarrollo de la comunicación política en la sociedad de la información global en sus obras: M.S. Vershinin, M. N. Grachev, S. A. Zelentsa, Yu. V. Irkhin, Yu. B. Yaashlev, Yu. Yu. Lectorov, E.A. Maksimova, O. A. Malalanov, M. G. Morozova, V. D. Popov, E. V. Protsentso, E. V. Rodionov, O. F. Rusaltsov, A. I. Solovev, L. P. Timofeev, A. Yu. Tsaplin, F. I. Zharkov (2009), y otros.

Expertos políticos como G. Almond, M. Castells, H. Lasswell, D. Lilleker y G. Powell, que publicaron en inglés, dedicaron sus obras al examen de los fundamentos metodológicos del estudio de la ciencia de la comunicación.

El concepto de seguridad de la información surgió a finales de los años 80 en la obra del científico alemán G. Odermann. Se refiere a un componente importante de la seguridad internacional y busca abordar de manera integral los problemas de seguridad relacionados con las amenazas de información. Hubo una tendencia a estudiar abiertamente el problema de la seguridad de la información como un tema independiente en la literatura científica de la Comunidad de Estados Independientes a fines de 1991, principios de 1992 (Lipkan, 2006).

Es importante destacar que no existe una opinión consolidada sobre el concepto de "seguridad de la información" en la literatura científica. Por ejemplo, Bogush (2005) entiende el concepto de seguridad de la información como la seguridad del entorno de información que cumple con los intereses nacionales, en el cual las amenazas de información internas y externas no influyen en la formación, uso y oportunidades de desarrollo. Kalyuzhny (2000) considera la seguridad de la información como un estado de seguridad del espacio de información, que garantiza su formación y desarrollo en interés del individuo, la sociedad y la nación. Zharkov (2009) entiende la seguridad de la información como el estado de disposiciones legales e instituciones de seguridad pertinentes que garantizan la disponibilidad constante de datos para la toma de decisiones estratégicas y la protección de los recursos de información del país. Kormych (2004) sostiene que la seguridad de la información es la protección de las normas establecidas por la ley, de acuerdo con las cuales tienen lugar los procesos de información en un país, asegurando las condiciones de existencia y desarrollo de la persona, la sociedad y el estado garantizados por la Constitución.

En su obra "Guerra de la Información", Winn Schwartau (1996) investiga las guerras de la información, las amenazas cibernéticas y el impacto de la información en los estados y las organizaciones. El autor analiza los aspectos tecnológicos, sociales y políticos de las guerras de la información y propone estrategias para garantizar la seguridad de la información. El libro "Ruleta Rusa: La Historia Interna de la Guerra de Putin contra América y la Elección de Donald Trump" de Michael Isikoff y David Corn (2018) explora la participación de Rusia en las elecciones estadounidenses de 2016 y el uso de operaciones de información para influir en la opinión pública y los procesos políticos. Proporciona una descripción detallada de las tácticas y estrategias utilizadas en el impacto de la información. Clarke y Knake (2011) consideran la creciente amenaza de la ciberguerra y el impacto de la información en la seguridad nacional en "Ciberguerra: La Próxima Amenaza a la Seguridad Nacional y Qué Hacer al Respecto". Los autores analizan ejemplos de ciberataques y operaciones de información, así como sugieren estrategias y recomendaciones para protegerse contra ellos.

Cavelty (2008) considera el papel de la comunicación en la seguridad de la información en el contexto de las relaciones civiles-militares. En su libro "Asegurando la Patria: Infraestructura Crítica, Riesgo y (In)Seguridad", la autora explora cómo interactúan y comparten información sobre amenazas cibernéticas y actividades de seguridad diferentes partes (civiles y militares). En su obra "Diplomacia Digital: Teoría y Práctica", otros investigadores importantes en el campo de la seguridad de la información, Bjola y Holmes (2015), discuten cómo los gobiernos utilizan tecnologías de comunicación para gestionar sus relaciones en la comunidad internacional y cómo estas tecnologías pueden usarse para contrarrestar las amenazas cibernéticas.

En el artículo "Estrategia de Comunicación para la Seguridad de la Información: De la Teoría a la Práctica", Henning Brown, Michelle Chen y Katarina Wolf discuten los aspectos metodológicos y prácticos del conjunto de herramientas de seguridad de la información, incluido el desarrollo de estrategias, la elección de canales y herramientas de comunicación, la evaluación de la efectividad y la gestión de riesgos. En el artículo "Estrategia de

Comunicación para la Seguridad de la Información para Construir en el Mundo Digital", Daniel Rohder y Steven Schneider consideran cómo las herramientas de seguridad de la información pueden utilizarse para construir confianza y mejorar las relaciones entre el gobierno, las empresas y los ciudadanos en un mundo digital.

La seguridad de la información es una propiedad y atributo de la sociedad de la información, la actividad y el resultado de la actividad humana dirigida a establecer seguridad en el ámbito de la información. La seguridad de la información es más bien un proceso que un estado, ya que debe tener en cuenta el futuro. Al mismo tiempo, los objetos de la seguridad de la información son la persona, la sociedad y el estado. Los sujetos de la seguridad de la información son la información en todas sus manifestaciones, incluyendo las fuentes de información, los mecanismos y medios de su creación, acceso, difusión y las consecuencias de su uso. Los sujetos también involucran normas legales y organizativas regulatorias y normas que determinan el orden de su formación, aplicación y terminación (Voitovy, 2019).

En su libro "Comunicar la Ciberseguridad: Por qué las Palabras Importan", Karin S. Johnson explora la importancia de la comunicación efectiva en la seguridad de la información. Ofrece consejos y estrategias prácticas para desarrollar planes de comunicación efectivos y mensajes relacionados con la seguridad de la información. En su artículo "Comunicación Estratégica para la Ciberseguridad: Una Taxonomía y Marco Analítico", David S. Wall revela los principios básicos y modelos de comunicación estratégica en el campo de la seguridad de la información. El autor ofrece una taxonomía y un marco analítico para comprender y aplicar estrategias de comunicación en ciberseguridad.

"Comunicaciones Estratégicas para la Seguridad Cibernética: Una Revisión Sistemática de la Literatura" de Isabel Wagner es una revisión de artículos científicos sobre comunicación estratégica en el campo de la ciberseguridad. Ella analiza la literatura existente y destaca temas clave, desafíos y estrategias de comunicación que pueden aplicarse en el contexto de la seguridad de la información.

Lo anterior indica que el significado y el contexto de la seguridad de la información son tan amplios y complejos que requieren la movilización de académicos de diferentes esferas de la ciencia. La formación del concepto de comunicaciones estratégicas ha pasado por tres etapas en el sistema de la OTAN:

1. Comunicaciones estratégicas = asuntos públicos: la función de liderar activamente las relaciones de la sociedad civil con las autoridades. Este enfoque es inherente a ciertas instituciones nacionales, pero no es un estándar común en la OTAN.

2. La comunicación estratégica es una batalla de narrativas (enfoque obsoleto de la OTAN).

3. Las comunicaciones estratégicas no son asuntos públicos, sino una forma integrada de acciones sistémicas en el espacio de la información (enfoque moderno de la OTAN).

El documento "Comunicación Efectiva en Ciberseguridad: Un Informe de Política" (Gobierno Australiano, 2016), desarrollado por el Gobierno Australiano, es muy interesante en el contexto de la comunicación efectiva en el campo de la ciberseguridad. Aborda la importancia de la comunicación efectiva en ciberseguridad y ofrece recomendaciones prácticas y ejemplos para mejorar los esfuerzos de comunicación en seguridad de la información.

Estos documentos académicos representan solo una pequeña parte de la literatura relacionada con la estrategia de comunicación para la seguridad de la información.

3. Seguridad de la información en la república de Kazajistán

La República de Kazajistán ocupa una posición líder en cuanto al acceso a las tecnologías de la información entre los países de Asia Central. La seguridad de la información en la República de Kazajistán es un elemento

importante destinado a garantizar la seguridad de los recursos de información y a proteger a los ciudadanos, organizaciones y organismos estatales de las ciberamenazas. Kazajistán es el primer país de Asia Central en adoptar documentos regulatorios que rigen las actividades de la comunidad de Internet. En 1997, el mensaje del Presidente "Prosperidad, seguridad y mejora del bienestar de todos los kazajos" presentó la estrategia de desarrollo de Kazajistán hasta 2030. Se establece que la seguridad nacional del país depende de la seguridad de la información (Mensaje del Presidente de la República de Kazajistán Nursultan Nazarbayev al pueblo de Kazajistán..., 2007).

Por lo tanto, se pueden distinguir algunas características de la seguridad de la información en Kazajistán:

Marco legislativo: La República de Kazajistán estableció el Instituto de Problemas de Informática y Gestión (2022) y adoptó actos legislativos fundamentales como "Sobre los Secretos de Estado" (Ley de la República de Kazajistán No. 349-I..., 1999) y "Programa Estatal para la Formación y Desarrollo de la Infraestructura Nacional de Información de la República de Kazajistán para 2001-2003" (2001).

Organismos estatales: El Comité de Seguridad de la Información bajo el Ministerio de Desarrollo Digital, Innovación e Industria Aeroespacial (2022) es responsable de la seguridad de la información en la República de Kazajistán. El Comité de Seguridad de la Información está encargado de desarrollar la cooperación internacional y medidas administrativas y técnicas, y de implementar la política estatal en el ámbito de la ciberseguridad, incluida la de mercado. Kazajistán cuenta con un Centro Nacional de Seguridad de la Información (NISC), que es responsable de coordinar y supervisar la seguridad de la información en el país. El NISC se encarga del análisis de amenazas, el desarrollo de políticas y estrategias, y la coordinación de actividades de seguridad de la información. Kazajistán presta especial atención a la ciberseguridad y las ciberamenazas. En el país se establecieron centros especiales para la detección y prevención de ciberataques. Además de eso, se organizan capacitaciones para mejorar las habilidades de los especialistas en el campo de la ciberseguridad.

Cooperación internacional: Kazajistán coopera activamente con socios internacionales en el ámbito de la seguridad de la información, incluidas las Naciones Unidas, la OSCE y otras organizaciones. Esta cooperación incluye el intercambio de información sobre amenazas cibernéticas, proyectos y programas conjuntos.

Educación y concienciación: En Kazajistán se presta atención a aumentar la alfabetización y la concienciación pública sobre la seguridad de la información. Se llevan a cabo programas educativos y capacitaciones para un público amplio y cursos especiales para especialistas en el campo de la seguridad de la información.

Hasta la fecha, en Kazajistán existen alrededor de 40 empresas, 19 centros de operaciones de seguridad privada (SOC), tres equipos de respuesta a emergencias informáticas (CERT), siete laboratorios privados de pruebas certificadas, ocho instituciones de educación superior y 25 instituciones de educación secundaria que se ocupan de cuestiones de ciberseguridad.

En los últimos años, Kazajistán ha elaborado enfoques básicos para el desarrollo de la ciberseguridad en el país. Uno de estos enfoques es el concepto "Cibershield de Kazajistán" (2017). Su objetivo es determinar las direcciones clave de la implementación de la política estatal en el campo de las tecnologías de la información y las telecomunicaciones, proteger los recursos de información electrónica, aumentar la alfabetización digital entre la población y las empresas, y garantizar el uso seguro de las tecnologías de la información y la comunicación. Una nueva versión del concepto "Cibershield de Kazajistán-2" se adoptará en la segunda mitad de 2022. En el marco de su implementación hasta 2027, se presentarán las principales direcciones para fortalecer la responsabilidad administrativa por la filtración de datos personales, el desarrollo de software doméstico, el uso de plataformas sociales y mediáticas de Kazajistán, y la regulación de las actividades de las extranjeras. Además, este documento considerará los desafíos y amenazas cibernéticas en el contexto de la experiencia internacional y las opiniones de expertos nacionales en el campo de la ciberseguridad.

Sin embargo, ya han entrado en vigor numerosas disposiciones legislativas y órdenes en el campo de la ciberseguridad. Además, se han establecido laboratorios de pruebas de seguridad de la información para la

investigación de códigos maliciosos, se ha puesto en marcha un centro nacional de coordinación de seguridad de la información, un equipo de respuesta a emergencias informáticas privado (CERT) y siete centros de operaciones de seguridad (SOC), y se ha aumentado el número de subvenciones en este campo.

Con el fin de mejorar la situación en el campo de la seguridad de la información y la protección de datos personales, el Ministerio de Desarrollo Digital, Innovación e Industria Aeroespacial de la República de Kazajistán planteó la cuestión de asignar al Comité de Seguridad de la Información las funciones de proteger los datos personales, llevar a cabo auditorías e inspecciones de los propietarios de sistemas de información para el procesamiento de datos personales.

El 21 de junio de 2021, el Presidente de la República de Kazajistán, Kassym-Jomart Tokayev, firmó un Decreto "Sobre la aprobación de la Estrategia Nacional de Seguridad de la República de Kazajistán para 2021-2025" (2021). La nueva Estrategia Nacional de Seguridad de la República de Kazajistán fue la sexta de su tipo en ser adoptada en el momento de la independencia. La Ley "Sobre la Seguridad Nacional de la República de Kazajistán" define la Estrategia como un documento estratégico para el desarrollo del estado, que determina los principales desafíos y amenazas, los objetivos estratégicos y los indicadores objetivos, así como los objetivos e indicadores de resultados en el campo de la seguridad nacional. Además, esta Estrategia es uno de los elementos del sistema de planificación nacional y se desarrolla en el contexto de la implementación de la Estrategia de Desarrollo de Kazajistán hasta 2050.

Kazajistán actualmente está en un curso para la formación y establecimiento de sus mecanismos de protección de la seguridad de la información. Para desarrollar la industria, primero es necesario realizar lo siguiente:

1. Diseñar canales educativos dedicados a las comunicaciones digitales y habilidades. Debe haber un equilibrio entre el contenido educativo y las lecciones y materiales aplicados destinados a desarrollar habilidades y potencial de empleo.

2. Desarrollar formatos de eventos temáticos para el intercambio de opiniones y el diseño participativo. De esta manera, se pondrán en servicio mecanismos extra-institucionales para los jóvenes y su diálogo con los tomadores de decisiones en todos los niveles.

3. Ampliar plataformas en línea y offline para la participación del público objetivo en actividades sociales y económicas, como la promoción de pasantías y oportunidades de capacitación a través de pasantías, el desarrollo de programas de mentoría, la mejora de la orientación profesional y el asesoramiento en escuelas y universidades, la expansión de oportunidades para el voluntariado y programas de verano.

4. Establecer fondos de solidaridad juvenil, que incluyan programas de pequeñas subvenciones, para promover iniciativas de lucha contra el extremismo violento a nivel comunitario, local o de base.

5. Desarrollar una industria de juegos móviles dirigida a la educación y la concienciación sobre la radicalización y sus consecuencias.

4. Seguridad de la información de Ucrania

La seguridad de la información ocupa un lugar especial en el sistema de seguridad nacional de Ucrania. Ucrania está trabajando activamente en el desarrollo e implementación de medidas y políticas estratégicas destinadas a garantizar la seguridad de la información y la protección contra las ciberamenazas. La provisión de seguridad de la información es una de las funciones gubernamentales esenciales en Ucrania, ya que el país ha experimentado ataques de información inusuales por parte de la Federación Rusa poco después de la Revolución de la Dignidad. Ucrania no había centrado su atención en la seguridad de la información durante 20 años de independencia, y el resultado fue la anexión de territorios y mentes desinformadas de personas en áreas fuera del control gubernamental.

Ucrania comenzó a hablar de manera más activa sobre comunicaciones estratégicas en 2014, cuando Rusia recurrió a la agresión armada. Un componente importante de esta última fue una campaña de desinformación, cuando la propaganda rusa llamó a Ucrania un estado fallido, inventando historias sobre "niños crucificados" y otras cosas. De esta manera, el Kremlin trató de mostrar al mundo que la "guerra civil" no se detuvo en el Donbás y que ucranianos y rusos eran "un solo pueblo".

A nivel institucional, numerosos organismos gubernamentales se encargan de la provisión de áreas específicas de seguridad de la información, a saber, el Ministerio de Política de Información, el Consejo Nacional y el Comité Estatal de Televisión y Radiodifusión de Ucrania, la Comisión Nacional para la Regulación Estatal de Comunicaciones e Informatización, el Ministerio de Asuntos Exteriores de Ucrania, el Ministerio del Interior de Ucrania, el Servicio de Seguridad de Ucrania y el Servicio Estatal de Comunicaciones Especiales y Protección de la Información de Ucrania. Se han creado divisiones para comunicaciones estratégicas en las estructuras gubernamentales y universidades de Ucrania. En particular, se trata del Centro de Investigación y Educación de Comunicaciones Estratégicas en el ámbito de la Seguridad Nacional y Defensa en la Universidad Nacional de Defensa de Ucrania, que lleva el nombre de Ivan Cherniakhovskyi, y la gestión de comunicaciones estratégicas del Estado Mayor del Comandante en Jefe de las Fuerzas Armadas de Ucrania.

La implementación de la política estatal en esta área está encomendada al órgano ejecutivo central, el Ministerio de Política de Información de Ucrania, que ha sido el principal organismo responsable de la seguridad de la información nacional desde 2015. Cabe destacar que uno de los éxitos del Ministerio de Política de Información es la adopción de la Doctrina de Seguridad de la Información de Ucrania (2017). El propósito de la Doctrina es aclarar las bases para la formación e implementación de la política estatal de información, principalmente para contrarrestar la influencia de la información destructiva de la Federación Rusa en el contexto de su guerra híbrida.

El Gabinete de Ministros de Ucrania aprobó la Estrategia de Seguridad de la Información (2021) el 15 de septiembre de 2021. Esta Estrategia es uno de los numerosos documentos desarrollados para implementar la Estrategia de Seguridad Nacional de Ucrania. Su propósito es establecer condiciones para garantizar la seguridad de la información de Ucrania, con el objetivo de proteger los intereses vitales de un ciudadano, la sociedad y el estado en la lucha contra amenazas internas y externas. La Estrategia también sienta las bases para la protección de la soberanía e integridad territorial de Ucrania, el apoyo a la estabilidad social y política, la seguridad nacional y la garantía de los derechos y libertades de cada ciudadano. La implementación de la Estrategia está planificada para el período hasta 2025.

El resultado esperado de la implementación de la Estrategia es un espacio de información seguro en Ucrania, que incluye la contrarrestación efectiva de contenidos ilegales, la promoción de un sistema eficaz de comunicaciones estratégicas y el fortalecimiento de la cultura mediática y la alfabetización mediática de la población. Sin embargo, su sección relevante sólo proporciona definiciones generales del estado deseado en caso de la implementación de la Estrategia. Una descripción más detallada del estado de las cosas en el campo de la seguridad de la información o indicadores cuantitativos y cualitativos particulares podrían informar mejor sobre la efectividad de la implementación de esta Estrategia. El Consejo de Seguridad y Defensa Nacional puede finalizar la estrategia de seguridad de la información antes de su aprobación por el Presidente de Ucrania. En general, es un documento marco y no brinda la oportunidad de evaluar hasta qué punto su implementación afectará el ejercicio de los derechos digitales. Es necesario considerar las siguientes nuances al desarrollar un plan de acción y legislación para la implementación de la Estrategia. Cualquier medida legislativa destinada a contrarrestar la desinformación y restringir el acceso a contenido perjudicial en Internet puede imponer limitaciones al derecho a la libertad de expresión sólo si cumplen

> "Daniel Rohder y Steven Schneider consideran cómo las herramientas de seguridad de la información pueden utilizarse para construir confianza y mejorar las relaciones entre el gobierno, las empresas y los ciudadanos en un mundo digital."

con los requisitos de legalidad y proporcionalidad. Las autoridades públicas involucradas en la implementación de la Estrategia deben tener una distribución clara de poderes y sus actividades deben ser transparentes. En particular, es necesario definir estrictamente el organismo encargado de la implementación de la Estrategia, que analizará y rendirá cuentas al público sobre la efectividad de las medidas tomadas para su implementación.

El Centro de Comunicaciones Estratégicas y Seguridad de la Información (2022) opera bajo el Ministerio de Cultura y Política de Información de Ucrania. El enfoque del trabajo del Centro es la contrarrestación de amenazas externas, la integración de esfuerzos del estado y organizaciones públicas en la lucha contra la desinformación, la respuesta rápida a noticias falsas y la promoción de narrativas ucranianas.

Los objetivos clave del Centro son los siguientes:

- Desarrollar comunicaciones estratégicas (contranarrativas de la Federación Rusa, campañas de información, inclusión de narrativas ucranianas la comunicación diaria del Gobierno).
- Contrarrestar y fortalecer la resiliencia contra la desinformación (notificar permanentemente los ataques de información contra Ucrania en los recursos del Centro, en particular en el portal web, la página de Facebook y el canal de Telegram).
- Aumentar la conciencia sobre las amenazas híbridas (diseñar y brindar capacitación para funcionarios públicos y representantes de unidades de comunicación, en particular).
- Informar regularmente sobre la agresión híbrida de Rusia a nivel internacional y desarrollar mecanismos para contrarrestar la desinformación con la ayuda de socios internacionales.

Para lograr este propósito, el Centro produce numerosos productos de información que incluyen:

1. Plataformas de comunicación del Centro (sitio web y páginas oficiales en redes sociales).
2. Cuadro de mensajes "Las principales posiciones de la respuesta informativa. Explicamos cosas complejas en palabras sencillas" (un análisis diario de los principales eventos y las tesis establecidas para su explicación. Estas tesis son útiles para el trabajo diario de políticos, funcionarios públicos, comunicadores de entidades gubernamentales, periodistas y expertos en otras categorías. Para diferentes audiencias).
3. Resumen diario "Cómo funciona la propaganda rusa en tiempos de guerra".
4. Resumen analítico, que se publica a diario y contiene una descripción de los materiales recopilados sobre la propaganda y las narrativas utilizadas en el espacio mediático de Rusia.
5. Una serie de productos bajo el nombre general de dovidka.info (un directorio actualizado "En caso de emergencia o guerra", el sitio web dovidka.info y chatbots con el envío diario de consejos y recomendaciones actualizados).
6. Elemento de capacitación para funcionarios públicos (cursos de capacitación dedicados a la desinformación, las noticias falsas y los fundamentos de la comunicación efectiva; charlas cortas y seminarios web sobre temas actuales, incluida la detección de noticias falsas en línea, la guerra híbrida y la propaganda).

Ucrania es el primer país en consagrar el concepto de comunicaciones estratégicas en actos oficiales, como la Doctrina Militar de Ucrania (Decreto del Presidente de Ucrania No. 47/2017, 2017), la Doctrina de Seguridad de la Información de Ucrania (Huberskyi, 2004) y la Estrategia de Seguridad de la Información de Ucrania (2021).

El plan de acción para la implementación de la Estrategia debe proporcionar indicadores claros para medir la efectividad de su implementación. Se debe garantizar la participación pública completa en lugar de meramente formal para implementar las disposiciones de la Estrategia y diseñar un plan de acción. Dado que Ucrania es un país ortodoxo y la iglesia ocupa un lugar significativo en la vida de los ucranianos, los activistas prorrusos continúan desinformando a la gente con la ayuda de la iglesia hasta el día de hoy, lo que complica la implementación de la estrategia de comunicación.

La provisión de la integridad territorial y la seguridad nacional como fundamentos de la unidad nacional de Ucrania requiere la implementación altamente efectiva de las disposiciones de la legislación vigente (normas legales) en las actividades de información de los funcionarios públicos. Lo anterior es posible sólo si se mejoran aún más los métodos y formas de administración pública de los sujetos del poder, su cultura legal y competencia profesional son elevadas, y la gobernanza electrónica en Ucrania se desarrolla aún más. Es necesario sistematizar y utilizar de manera algorítmica mecanismos para garantizar la seguridad de la información interna y formar el apoyo a Ucrania en las sociedades de los países socios a través de la dominación de la información en su territorio, la represión efectiva de los ataques de información rusos y el desarrollo de contenido de alta calidad para acceder a los espacios de información externa.

Ucrania presta atención a mejorar la alfabetización en información y la conciencia de los ciudadanos sobre la seguridad de la información. Se llevan a cabo campañas educativas, seminarios y capacitaciones para aumentar la conciencia sobre las amenazas cibernéticas, la seguridad en línea y el comportamiento correcto en el espacio digital. En general, Ucrania está desarrollando y mejorando activamente las capacidades de seguridad de la información para proteger sus recursos de información, ciudadanos e infraestructura crítica de amenazas cibernéticas.

5. Política de seguridad de la información en la UE

La Política de Seguridad de la Información en la Unión Europea se basa en el deseo de proporcionar un alto nivel de protección de la información y los datos para respaldar la seguridad de los ciudadanos, las empresas y los Estados miembros de la UE. La UE ha tomado una amplia gama de medidas e iniciativas para fortalecer la seguridad de la información a nivel regional. La Unión Europea lleva a cabo una política activa de seguridad de la información. En 2001, la Comisión Europea presentó el primer documento titulado "Seguridad de Red y de la Información: Propuesta para un Enfoque de Política Europea", que delineó un enfoque europeo para los temas de seguridad de la información. El documento utiliza el término "seguridad de red e información", interpretado como la capacidad de una red o un sistema de información para resistir eventos accidentales o acciones maliciosas que representan una amenaza para la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos, así como los servicios relacionados ofrecidos a través de estas redes y sistemas (Comunicación de la Comisión Europea: Seguridad de Red y de la Información: Propuesta para un Enfoque de Política Europea, 2001).

El documento define las siguientes direcciones principales de la política de seguridad de la información en Europa:

1. Aumentar la conciencia de los usuarios sobre las posibles amenazas al utilizar redes de comunicación. Las actividades prioritarias en este ámbito incluyen campañas públicas de información y educación, la promoción de las mejores prácticas en seguridad y el desarrollo de cursos de formación sobre cuestiones de seguridad.

2. Establecer un sistema europeo de advertencia e información. La principal tarea de los países de la UE es diseñar un mecanismo confidencial para la notificación de ataques a entidades comerciales y un sistema de alerta para los usuarios que informe sobre el peligro y ofrezca consejos para contrarrestar los ataques. Con este fin, los Estados miembros deben revisar el soporte técnico y la competencia de los equipos de respuesta a incidentes informáticos (CERT) nacionales y mejorar la cooperación entre los equipos de respuesta a incidentes informáticos y estructuras similares en otros países.

3. Garantizar el apoyo tecnológico. La investigación en seguridad de redes e información es prioritaria. Para lograr este propósito, el Programa Marco de Investigación de la UE debe abordar cuestiones de seguridad, y se alienta a los Estados miembros a promover el uso activo del cifrado variable.

4. Apoyar la estandarización y la certificación orientadas al mercado. La existencia de numerosas normas y especificaciones competitivas en el campo de la seguridad de la información es el principal problema en la UE, lo que conduce a la fragmentación del mercado y soluciones incompatibles. La solución propuesta para este problema implica la revisión de las normas de seguridad existentes, el desarrollo de productos y servicios compatibles y seguros, y la promoción del uso de procedimientos de certificación y acreditación de acuerdo con normas europeas e internacionales ampliamente aceptadas.

5. Proporcionar apoyo legal. Las direcciones prioritarias de la política de la UE en el campo de la regulación legal de la seguridad de la información son la protección de datos personales, los servicios de telecomunicaciones y la ciberdelincuencia. También implican el establecimiento de condiciones favorables para la libre circulación de productos y servicios de cifrado por parte de los Estados miembros mediante la armonización de procedimientos de exportación administrativa y la relajación de los controles de exportación.

6. Fortalecer la seguridad a nivel estatal. La cuestión de la seguridad es esencial para el desarrollo continuo de la administración electrónica. La principal tarea de las autoridades estatales es promover el desarrollo de una cultura de seguridad. En este ámbito, se prevé la introducción de medios eficaces y compatibles de seguridad de la información y se alienta a los Estados miembros a utilizar firmas electrónicas al proporcionar servicios públicos en línea.

7. Desarrollar la cooperación internacional en el ámbito de la seguridad de la información. La tarea principal de la UE es reforzar el diálogo de la Comisión Europea con organizaciones internacionales y socios sobre el problema de la seguridad de las redes y, en particular, la creciente dependencia de las redes electrónicas.

La Agencia Europea de Seguridad de las Redes y de la Información se estableció el 10 de marzo de 2004. Su propósito es fortalecer las capacidades de la comunidad europea, los Estados miembros y la comunidad empresarial para prevenir y responder a cuestiones relacionadas con la seguridad de la información. Las principales áreas de actividad de la Agencia son las siguientes: proporcionar servicios de asesoramiento y asistencia a la Comisión y a los Estados miembros en el ámbito de la seguridad de la información; recopilar y analizar datos sobre incidentes de seguridad en Europa y riesgos emergentes; diseñar técnicas de evaluación y gestión de riesgos para mejorar la respuesta de la UE a las amenazas a la seguridad de la información; fomentar la concienciación y promover la cooperación entre los distintos actores en el ámbito de la seguridad de la información estimulando la interacción entre los sectores público y privado. La Agencia también presta asistencia a la Comisión Europea en trabajos técnicos preliminares para actualizar y mejorar la legislación europea en el ámbito de la seguridad de las redes y la información.

La UE presta una atención significativa a la ciberseguridad como componente de la seguridad de la información. La UE ha estado implementando programas de Internet más seguros desde 1999. Cada programa tiene una duración de 4 a 5 años. El Programa de Internet más seguro para 2009-2013 presupone numerosas medidas para combatir el contenido malicioso y el comportamiento peligroso en Internet. Los objetivos principales del programa son concienciar al público, proporcionar al público una red de puntos de contacto para denunciar contenido y comportamiento ilegal y perjudicial, promover iniciativas de autorregulación en esta área e involucrar a los niños en el diseño de un entorno en línea más seguro, y desarrollar una base de conocimientos sobre las nuevas tendencias en tecnologías en línea y sus consecuencias para la vida de los niños. Los aspectos clave de la política de seguridad de la información en la UE son los siguientes:

Legislación y regulación: La UE desarrolla y adopta regulaciones destinadas a garantizar la seguridad de la información. Por ejemplo, el Reglamento General de Protección de Datos (RGPD) establece normas para el procesamiento y la protección de datos personales en la UE.

Cooperación y coordinación: la UE apoya la cooperación y coordinación entre los Estados miembros en el ámbito de la seguridad de la información. Esto incluye compartir información sobre amenazas cibernéticas, ejercicios de preparación y mecanismos de respuesta a ciberataques.

Ciberseguridad y protección de infraestructuras críticas: la UE está desarrollando medidas y normas para proteger la infraestructura de información crítica, como sistemas de energía, redes de transporte e instituciones financieras, de las amenazas cibernéticas.

Investigación e innovación: la UE apoya la investigación y el desarrollo en el campo de la seguridad de la información. Se financian proyectos e iniciativas para desarrollar nuevas tecnologías y soluciones en el campo de la ciberseguridad.

Fomento de la cultura de la información: la UE tiene como objetivo aumentar la alfabetización informática y la conciencia entre los ciudadanos, las empresas y las autoridades. Se están implementando programas educativos y campañas informativas para concienciar sobre las amenazas y promover un comportamiento seguro en el espacio digital.

Cooperación internacional: la UE coopera activamente con socios y organizaciones internacionales en el ámbito de la seguridad de la información. Se establecen asociaciones para compartir información, coordinar respuestas a amenazas cibernéticas y desarrollar normas y estándares internacionales.

La adopción de la Comunicación de la Comisión Europea "Estrategia para una Sociedad de la Información Segura: Diálogo, Asociación y Empoderamiento" (2006) fue un avance significativo en el desarrollo de políticas europeas en este ámbito. La Estrategia proporciona una visión general del estado actual de las amenazas a la seguridad de la sociedad de la información e identifica medidas de seguridad adicionales. En 2016, la UE acordó los principioTRs paneuropeos de seguridad de la información. El Parlamento Europeo aprobó una nueva directiva que enumeraba los sectores de la economía (energía, transporte, servicios bancarios) que tendrían que garantizar su capacidad para prevenir ciberataques. Además, las empresas están obligadas a informar a las autoridades nacionales en caso de un incidente grave de seguridad de la información. Los proveedores de servicios digitales como Amazon o Google deben facilitar el intercambio de información (Directiva sobre la Seguridad de los Sistemas de Red e Información, 2016).

La UE necesita implementar numerosas medidas para responder adecuadamente a los desafíos de ciberseguridad existentes:

1. Asegurar un nivel adecuado de formación en todos los niveles. Los Estados miembros deberían identificar capacidades básicas para los equipos nacionales de respuesta a incidentes informáticos y sistemas de respuesta a incidentes de seguridad. Esto implica también fortalecer la cooperación entre los sectores público y privado y establecer un foro europeo para el intercambio de información entre los Estados miembros.

2. Establecer un sistema europeo de alerta temprana de ciberataques.

3. Reforzar los mecanismos de seguridad de la infraestructura de información crítica de la UE, desarrollar planes nacionales de respuesta de emergencia y relaciones institucionales, llevar a cabo una formación paneuropea sobre incidentes de seguridad en Internet y mejorar la cooperación entre los equipos nacionales de respuesta a incidentes informáticos.

4. Desarrollar directrices europeas sobre la sostenibilidad y estabilidad de Internet y promoverlas en el ámbito internacional.

5. Determinar los criterios para identificar la infraestructura crítica de Europa en el sector de tecnologías de la información y comunicación.

Tanto las autoridades públicas como las organizaciones no gubernamentales deben implementar las prioridades políticas definidas por los órganos rectores de la Unión Europea en el ámbito de la seguridad de la información a nivel nacional.

Los enfoques desarrollados en la Unión Europea para garantizar la seguridad de la información reflejan la libertad acordada de los Estados miembros de la UE y las instituciones, y representan estándares marco europeos en esta área. Los países mencionados pueden aplicar con éxito estos estándares en caso de que se adapten a las particularidades de los sistemas legales estatales y a las características socioculturales.

La política de seguridad de la información de la UE es dinámica y evoluciona para adaptarse al entorno cibernético en constante cambio y proteger los intereses de los ciudadanos y las organizaciones en la UE.

6. Recomendaciones para el desarrollo de comunicaciones estratégicas

La Estrategia de Comunicación para la Seguridad de la Información es, de hecho, una herramienta importante para contrarrestar la guerra híbrida. La guerra híbrida es una combinación de diferentes métodos, que incluyen operaciones de información, ciberataques y manipulación de la opinión pública, con el fin de alcanzar objetivos políticos y militares. La experiencia mundial demuestra que una estrategia de comunicación efectiva para la seguridad de la información debe incluir los siguientes componentes:

1. Análisis y evaluación de vulnerabilidades: Es importante analizar las vulnerabilidades de la información e identificar posibles amenazas. Esto permitirá el desarrollo de medidas adecuadas para proteger la información.

2. Gestión de crisis: Se deben desarrollar planes de gestión de crisis que incluyan medidas para detectar, responder y recuperarse de ataques a la información. Una respuesta rápida y adecuada a los incidentes ayudará a minimizar sus consecuencias.

3. Comunicación pública: Es importante establecer un diálogo abierto y confidencial con el público. Esto se puede lograr a través de campañas de información, conferencias de prensa, recursos en Internet y redes sociales. Las organizaciones gubernamentales y no gubernamentales deben proporcionar información confiable sobre la situación actual, las amenazas y las medidas tomadas.

4. Cooperación internacional: La guerra híbrida a menudo tiene un carácter transfronterizo, por lo que es importante desarrollar la cooperación internacional en el ámbito de la seguridad de la información. El intercambio de experiencias, la coordinación de medidas y los esfuerzos conjuntos permiten hacer frente de manera más efectiva a las amenazas híbridas.

5. Enfoque integrado: La estrategia de comunicación debe formar parte de un enfoque integrado para la seguridad de la información. Debe interactuar con medidas de protección técnica, capacitación del personal, legislación y otros aspectos de la seguridad de la información.

La estrategia de comunicación debe centrarse en el sistema de parámetros de la audiencia objetivo, que incluye la conciencia cultural de los valores, normas y creencias actuales e históricos reflejados en varias estructuras sociales o su influencia en los motivos, intenciones y comportamiento de la audiencia objetivo (Plotnikova, 2011). La estrategia de comunicación también debe tener en cuenta la situación psicológica existente, es decir, el estado emocional, la mentalidad y otras motivaciones de comportamiento de la audiencia objetivo. Estas motivaciones de comportamiento se basan principalmente en características nacionales, políticas, sociales, económicas y psicológicas, pero las circunstancias y los eventos también pueden influir en ellas.

El enfoque para la formación de la estrategia debe hacer lo siguiente:

- Ser adaptativo y flexible, es decir, considerar las capacidades y necesidades de todos los participantes en la comunicación.
- Considerar los posibles riesgos para la toma de decisiones efectivas en equilibrar estos riesgos y beneficios.
- Basarse en el análisis del entorno de información, en una evaluación profunda de la situación y en la previsión para tomar decisiones efectivas.
- Estar centrado en la comunicación e interacción entre todos los actores de la comunicación estratégica para garantizar la comprensión mutua y la unidad de propósito y acción.

Es necesario calcular la eficacia de la audiencia objetivo, es decir, su capacidad para implementar la reacción o comportamiento deseado, ya sea el suyo propio o el de otros, como resultado de la implementación de la estrategia. La estrategia debe ser flexible, es decir, fácilmente adaptable a los requisitos cambiantes. Estos requisitos pueden ser previsibles e imprevisibles y pueden afectar, por ejemplo, la configuración, la aplicación, la ubicación o el uso de ciertos materiales informativos. Las acciones previstas por la estrategia deben estar sincronizadas, es decir, coordinadas en tiempo y espacio.

La innovación no es algo que deba temerse. A menudo, la innovación se percibe como una amenaza para el potencial existente y las inversiones. Dado que la innovación siempre está sujeta a dudas, a menudo significa la preparación para posibles conflictos (Nota Conjunta de Concepto 1/17 Concepto de Futuro de la Fuerza, 2017). En los últimos años, han tenido lugar numerosos eventos que demuestran que es posible perder la confianza de la audiencia objetivo o fortalecerla con comunicaciones estratégicas efectivas en cuestión de horas en el mundo.

Las comunicaciones estratégicas son una herramienta efectiva para hacer frente a amenazas híbridas. Su efectividad se determina mediante la implementación de un algoritmo de acciones proporcionado por el sistema, que incluye los siguientes pasos:

1. Análisis - monitoreo - evaluación del entorno de información y de las amenazas híbridas. El desarrollo del sistema de Comunicaciones Estratégicas implica actividades de investigación y análisis preliminares que se resuelven en el sistema de "análisis - monitoreo - evaluación". Esto implica el procesamiento de datos estructurados obtenidos de diversas fuentes para identificar objetos, conexiones y formas de comportamiento en el proceso de realización de eventos influyentes. En esta etapa, las autoridades políticas, militares y civiles deben consultar con expertos de la sociedad civil para coordinar posiciones y desarrollar recomendaciones para la introducción de las Comunicaciones Estratégicas.

2. Desarrollo de un concepto estratégico. Un concepto estratégico significa "un curso flexible de acciones adoptado como resultado de la evaluación de la situación estratégica para formar la estructura y el contenido de medidas militares, diplomáticas, económicas, psicológicas y otras medidas relevantes de las Comunicaciones Estratégicas" (Glosario de Términos y Definiciones de la OTAN, Oficina de Estandarización de la OTAN, 2014).

3. Desarrollo de un relato estratégico nacional y su difusión sistemática a diversas audiencias objetivo a través de todos los componentes de las Comunicaciones Estratégicas, incluyendo relaciones públicas, diplomacia pública, cooperación civil-militar, suministro de información y software. Este proceso debe ir acompañado de las siguientes acciones:

    - Desarrollar narrativas institucionales (operativas/tácticas) que respalden la narrativa estratégica y la detallen para una audiencia objetivo específica.

    - Mantener una narrativa estratégica a través de la difusión de contenido estratégico a través de diferentes canales de comunicación, teniendo en cuenta el perfil de una audiencia objetivo en particular.

- Desarrollar mecanismos de coordinación entre todos los actores de las comunicaciones estratégicas. Esto implica identificar la audiencia objetivo, es decir, los destinatarios de las narrativas y mensajes, y diseñar un algoritmo para comunicar los mensajes principales a representantes de las fuerzas de defensa y seguridad de diferentes rangos y a todas las audiencias objetivo en los componentes de las Comunicaciones Estratégicas.

4. Determinación de la efectividad de las actividades de comunicación estratégica que incluyen indicadores que reflejan un aumento o disminución en actividades específicas de la audiencia objetivo. Los indicadores ayudan a analizar y demostrar la efectividad de las actividades de acuerdo con las Comunicaciones Estratégicas. Una vez que se mide la efectividad, son posibles ajustes al concepto estratégico y su plan de implementación.

5. Considerar el contexto y la cultura: Al diseñar estrategias de comunicación y mensajes, considerar el contexto y la cultura de su audiencia. Adapte su lenguaje, imágenes y símbolos para que sean comprensibles y relevantes para su audiencia.

6. Prestar atención a la comunicación bidireccional: No olvidar la importancia de la comunicación bidireccional. Establecer mecanismos de retroalimentación, llevar a cabo encuestas e investigaciones para comprender las opiniones y necesidades de su audiencia. Esto ayudará a personalizar mejor sus estrategias de comunicación y mejorar la interacción con la audiencia.

7. Educar a los profesionales de la comunicación: Invertir en la formación y desarrollo de profesionales de la comunicación. Los comunicadores seguros y competentes podrán representar efectivamente a su organización y alcanzar los objetivos de comunicación.

8. Medir y evaluar resultados: Establecer métricas y un sistema para evaluar la efectividad de sus esfuerzos de comunicación. Medir los resultados permitirá determinar el éxito de sus estrategias y realizar los ajustes necesarios.

Para lograr una comunicación efectiva, es necesario construir modelos y formas de cooperación entre las partes interesadas y entre ellas y otros posibles socios. Al expandir la red de alianzas potenciales, aumentamos el poder de influencia y la difusión de mensajes favorables. Es importante recordar que la comunicación estratégica es un proceso continuo y que debe ser flexible y adaptable a las circunstancias cambiantes y a las necesidades de su audiencia.

7. Conclusiones

La manipulación dirigida de la opinión pública con tecnologías de lavado de cerebro es una de las manifestaciones más peligrosas de la guerra híbrida, que el estado agresor implementa contra el oponente. La seguridad de la información es una característica de un sistema de administración pública estable y sostenible, que mantiene sus componentes vitales cuando se enfrenta a amenazas internas y externas. En otras palabras, la seguridad de la información se encarga de proteger los intereses de los ciudadanos y del estado en el entorno de la información de diversas amenazas reales o virtuales.

Es importante señalar que las políticas de seguridad de la información varían de un país a otro, según sus necesidades, características y nivel de desarrollo.

Después de la Revolución de la Dignidad, Ucrania se convirtió involuntariamente en un participante en la guerra híbrida, lo que la obligó a pensar en la seguridad de la información y la comunicación con las áreas ocupadas en el menor tiempo posible. El resultado es una estrategia de comunicación competente, aunque tardía, para la seguridad de la información.

El concepto de seguridad de la información para Kazajistán se revela a través de la estrategia de su existencia como un estado soberano y estable, así como el desarrollo y la implementación de una política sistemática y equilibrada para proteger los intereses nacionales de amenazas de información externas e internas.

La Unión Europea otorga gran importancia a la seguridad de la información, ya que la considera esencial para el desarrollo exitoso de la sociedad de la información. La naturaleza transfronteriza de las amenazas de información exige la implementación de un conjunto de medidas a nivel paneuropeo, la armonización de sistemas nacionales para contrarrestar estas amenazas y el desarrollo de la cooperación entre organismos nacionales y europeos en la Unión Europea.

Las instituciones especializadas de la UE (Europol, Eurojust, la agencia ENISA) para la coordinación y el apoyo informativo y analítico de las actividades de las autoridades nacionales de aplicación de la ley y otros organismos complementan las actividades de las instituciones centrales de la UE (la Comisión Europea, el Parlamento Europeo y el Consejo de la UE) para el desarrollo de una estrategia y el fortalecimiento del marco legal para contrarrestar las amenazas a la seguridad de la información. La actividad de las instituciones y organismos de la UE en el ámbito de la seguridad de la información es más pronunciada en el antiguo primer pilar (Comunidad Europea) y tercer pilar (cooperación entre la policía y los tribunales penales). Sin embargo, no se observa un trabajo sistemático en el segundo pilar (política exterior y de seguridad común).

Las asociaciones público-privadas en esta área atraen una atención significativa, al igual que la participación de instituciones de la sociedad civil y del sector empresarial en actividades de seguridad de la información a nivel nacional y paneuropeo.

8. Referencias

Australian Government. (2016). *Australia's cyber security strategy. Enabling innovation, growth & prosperity.* https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf

Belkin, L., Iurynets, Ju., Sopilko, I., & Belkin, M. (2022). Culture and the use of information understanding in the field of national security (a case study of Ukraine). *Journal of International Legal Communication, 5*(2), 36-58. https://doi.org/10.32612/uw.27201643.2022.5.pp.36-58

Bjola, C., & Holmes, M. (2015). *Digital Diplomacy: Theory and Practice*. Routledge.

Bogush, V. (2005). *Information security of the state*. Kyiv: MK-Press.

Cavelty, M. D. (2008). *Securing the Homeland: Critical Infrastructure, Risk, and (In)Security*. Routledge.

Center for Strategic Communications. (2022). https://spravdi.gov.ua/pro-nas/

Clarke, R. A, & Knake, R. (2011). *Cyber War: The Next Threat to National Security and What to Do About It*. Ecco.

Decree of the President of the Republic of Kazakhstan. (2021). *On approval of the National Security Strategy of the Republic of Kazakhstan for 2021-2025*. https://acortar.link/zNFD2C

Decree of the President of the Republic of Kazakhstan No 573 (2001). *State program for the formation and development of the national information infrastructure of the Republic of Kazakhstan for 2001-2003*. https://adilet.zan.kz/rus/docs/U010000573_

Decree of the President of Ukraine No. 47/2017. (2017). *On the Doctrine of Information Security of Ukraine*. http://www. president.gov.ua/documents/472017-21374

Decree of the President of Ukraine No. 685/2021. (2021). *Information security strategy of Ukraine*. https://zakon.rada.gov.ua/laws/show/685/2021#Text

Decree of the President of Ukraine No. 685/2021. (2021). *On the decision of the National Security and Defense Council of Ukraine from 2021 "On Information Security Strategy"*. https://acortar.link/j6CHnH

Directive on Security of Network and Information Systems. (2016). E*urope agrees cyber threat strategy, plans to help fund more startups*. https://acortar.link/XG7Fqx

Huberskyi, L. V. (2004). *Ukrainian diplomatic encyclopedia*. Kyiv: Knowledge of Ukraine.

Information Security Committee under the Ministry of Digital Development, Innovation and Aerospace. (2022). https://www.gov.kz/memleket/entities/infsecurity?lang=ru

Institute for Informatics and Control Problems. (2022). https://iict.kz/ru/istoria-instityta/

Isikoff, M., & Corn, D. (2018). *Russian Roulette: The Inside Story of Putin's War on America and the Election of Donald Trump*. Twelve.

Kalyuzhny, R. (2000). The issue of the concept of reforming information legislation of Ukraine. *Collection Legal, normative and metrological support of the information protection system in Ukraine*, 17-21.

Kordunian, I. (2022). Establishment of the institute of mediation in Ukraine at the legislative level. *Journal of International Legal Communication, 5*(2), 108-116. https://doi.org/10.32612/uw.27201643.2022.5.pp.108-116

Kormych, B. A. (2004). *Information security: organizational and legal foundations*. Kyiv: Condor.

Law of Republic of Kazakhstan No 349-I (1999). *About state secrets*. https://online.zakon.kz/Document/?doc_id=1012633

Lipkan, V.A. (2006). *Information security of Ukraine in the conditions of European integration*. Kyiv: KNT.

MCM-0085-2010 STRATCOM. NATO. (2010). *Military Concept for Strategic Communications*. https://info.publicintelligence.net/NATO-STRATCOM-Concept.pdf.

Message of the President of the Republic of Kazakhstan N.Nazarbayev to the people of Kazakhstan (Part III). (2007). *Strategy "Kazakhstan-2030" at the New Stage of Development of Kazakhstan. 30 most important directions of our domestic and foreign policy*. https://online.zakon.kz/Document/?doc_id=30090778&pos=2;-106#pos=2;-106

NATO Glossary of Terms and Definitions. (2014). *North Atlantic Treaty Organization NATO Standardization Office (NSO)*. wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6EN.pdf

Oxford English Dictionary. (2022). *Post-truth.* http://www.oed.com

Plotnikova, S. (2011). *Technologization of discourse in modern society*. Iruktsk: IGLU.

Safer Internet Programme. (1999). http://ec.europa.eu/information_society/activities/sip/policy/programme/current_prog/index_en.htm

Schwartau, W. (1996). *Information Warfare*. Thunder's Mouth Press.

Sopilko, I. (2022). Cyber threat intelligence as a new phenomenon: legal aspect. *Journal of International Legal Communication, 4*(1), 8-18. https://doi.org/10.32612/uw.27201643.2022.1.pp.8-18

Cyber Shield of Kazakhstan. (2017). https://adilet.zan.kz/rus/docs/P1700000407

The European Network and Information Security Agency. (2022). http://www.enisa.europa.eu/

Voitovy, R. (2019). *Information security: approaches to defining the concept*. https://n9.cl/a1w4b

Zharkov, Y. M., & Besedina, L. M. (2009). Directions of external informational and psychological influence on Ukraine. *Collection of Scientific Works of the Military Institute of T. Shevchenko National University of Kyiv*. http//www.nbuv.gov.ua/portal/natural/znpviknu/2009-19/vip19-21.pdf

9. Artículos relacionados

Agudelo González, L. E., Marta-Lazo, C., & Aguaded, I. (2022). Competencias digitales en el Currículo de Periodismo: Análisis de caso de una universidad Centroamericana. *Vivat Academia. Revista de Comunicación*, 155, 297-316. https://doi.org/10.15178/va.2022.155.e1393

Aladro Vico, E. (2020). Comunicación sostenible y sociedad 2.0: particularidades en una relación de tres décadas. *Revista de Comunicación de la SEECI*, 53, 37-51. https://doi.org/10.15198/seeci.2020.53.37-51

Carrera, P., Blanco-Ruiz, M., & Sainz-de-Baranda Andújar, C. (2020). Consumo mediático entre adolescentes. Nuevos medios y viejos relatos en el entorno transmedia. *Historia y Comunicación Social, 25*(2), 563-574. https://doi.org/10.5209/hics.72285

Conde del Río, M. A. (2021). Estructura mediática de Tiktok: estudio de caso de la red social de los más jóvenes. *Revista de Ciencias de la Comunicación e Información*, 26, 59-77. https://doi.org/10.35742/rcci.2021.26.e126

López-Borrull, A. (2022). Invasión rusa en Ucrania: análisis desinformativo de la primera semana de conflicto. *COMeIN*, 119. https://doi.org/10.7238/issn.2014-2226

CONTRIBUCIONES DE LOS AUTORES, FINANCIAMIENTO Y AGRADECIMIENTOS

Contribuciones de los Autores: Las contribuciones de los autores son iguales.

Financiamiento: Los autores no recibieron apoyo de ninguna organización para el trabajo presentado. No se recibieron fondos, subvenciones ni ningún otro tipo de apoyo.

Conflictos de Intereses: Los autores declaran que no tienen intereses financieros ni conflictos de intereses competitivos.

AUTORES:

Arailym Nussipova
Doctor en Ciencias Sociales. Departamento de Kazakh-American University International Educational Corporation 050043, 28 Ryskulbekova Str., Almaty, República de Kazajstán.

arailym_nussipova@sci-academy.cc

Orcid ID: https://orcid.org/0000-0002-4112-1971
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57693920100

Gulzhan Khussainova
Doctor en Filosofía y Profesor Asociado. Departamento de Disciplinas Sociales y Políticas K. Zhubanov Universidad Regional de Aktobe 030000, Avenida A.Moldagulova 34, Aktobe, República de Kazajstán.
gulzhan_khussainova@un-nyc.net

Orcid ID: https://orcid.org/0000-0002-8893-1517

Raushangul Kabilova
Doctor en Filosofía y Profesor Asociado. Departamento de la Corporación Educativa Internacional de la Universidad Kazajo-Americana 050043, 28 Ryskulbekova Str., Almaty, República de Kazajstán.
raushangul_kabilova@sci-academy.cc

Orcid ID: https://orcid.org/0000-0001-8017-4868

Esenzhol Aliyarov
Doctor en Ciencias Políticas y Profesor. Asociación de Estudios Políticos 500500, Avenida Abay 68/74, Almaty, República de Kazajstán.
esenzhol_aliyarov@pltch-sci.com

Orcid ID: https://orcid.org/0000-0002-4173-7100
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57579013900

Botakoz Nuralina
Máster en ciencias humanitarias y profesor asistente. Departamento de la Universidad Kazajo-Americana Corporación Educativa Internacional 050043, 28 Ryskulbekova Str., Almaty, República de Kazajstán.
botakoz_nuralina@sci-academy.cc

Orcid ID: https://orcid.org/0000-0002-7634-522X