Infraestructura Critica

A Preprint

Grupo Messi *
Universidad Nacional de Cuyo

Mendoza Argentina

June 17, 2024

Abstract

Las infraestructuras críticas son elementos esenciales y vulnerables que, de ser perturbados, tendrían un impacto grave en los servicios esenciales. La protección de estas infraestructuras es crucial para prevenir ataques terroristas, lo que requiere medidas de protección física, ciberseguridad y cooperación internacional. En el caso específico del Puerto de Buenos Aires, se destaca la importancia de un enfoque integral y personalizado para garantizar su seguridad ante posibles amenazas.

1 Infraestructuras Críticas

Se entiende por infraestructuras críticas a las instalaciones estratégicas cuyo funcionamiento es indispensable y no admiten soluciones alternativas. Su perturbación, interrupción, interferencia o destrucción tendría un grave impacto sobre los servicios esenciales. Toda acción, deliberada o no, que atente contra el normal desempeño de suministros como electricidad, agua, gas, Internet; transporte público (trenes, autobuses de corta, media y larga distancia, metro/subte, vuelos, medios fluviales o marítimos), cadena logística y de distribución, etc. Supone eventos del mundo físico tales como vandalismo, sabotaje, allanamientos, fenómenos meteorológicos, terremotos, tsunamis, huracanes; o transacciones del universo virtual. El quinto dominio representado por el ciberespacio se ha convertido en un territorio donde se llevan a cabo batallas asimétricas en las que desde un simple internauta hasta un poderoso Estado-Nación pueden infligir daños de consideración a las infraestructuras críticas.

Las redes de infraestructura constituyen un elemento central de la integración del sistema económico y territorial de los países.

Una infraestructura adecuada es un factor explicativo importante de la capacidad de los países de diversificar sus economías, expandir el comercio, responder al crecimiento demográfico, reducir la pobreza y mejorar sus condiciones medioambientales.

Los debates respecto a la continuidad de los servicios de infraestructura han adquirido mayor relevancia tras la eclosión de combinaciones más complejas de peligros, y el aumento de la frecuencia y magnitud de eventos extremos con grandes impactos sobre los sistemas de transporte, energía, viviendas y servicios de infraestructura social. La pandemia del COVID-19, por ejemplo, ha evidenciado la necesidad urgente de garantizar que, en escenarios de crisis y cambios drásticos de patrones de consumo, la infraestructura sea capaz de facilitar la provisión fluida de servicios de transporte, conectividad y servicios públicos.

No obstante ello, son relativamente pocos los países que los utilizan, de forma sistemática, instrumentos para analizar y mitigar los riesgos que se ciernen sobre la infraestructura.

*Ingeniero Ricardo Palma

2 El rol de la infraestructura en el desarrollo

El rol fundamental que cumple la infraestructura en el proceso de desarrollo ha sido ampliamente reconocido y analizado en la literatura. Según el Besant-Jones y otros (1994), una infraestructura adecuada es un factor explicativo importante de la capacidad de los países de diversificar sus economías, expandir el comercio, responder al crecimiento demográfico, reducir la pobreza y mejorar sus condiciones medioambientales.

Las redes de infraestructura constituyen un elemento central de la integración del sistema económico y territorial de los países.

Se argumenta que la provisión adecuada de infraestructura tiene efectos positivos sobre la productividad de una economía y está asociada a la reducción de los costos de producción.

Con respecto a los vínculos entre la oferta de infraestructura y el crecimiento económico, a su vez, hay evidencias de una fuerte correlación entre ambas variables, aunque no sean inequívocos el grado y la dirección de la causalidad. Se asume, por lo tanto, que la dinámica de la inversión en infraestructura y el crecimiento económico se refuerzan mutuamente. Por otra parte, niveles insuficientes de inversión en infraestructura son identificados como una de las principales causas del bajo crecimiento económico en los países en desarrollo.

Como recalcan Fay y otros (2011), los vínculos entre infraestructura y desarrollo no son, necesariamente, inmediatos y unívocos. Además de la variedad de canales por medio de los cuales la oferta de infraestructura económica se puede convertir en condiciones socioeconómicas favorables, dichos efectos pueden variar significativamente entre países y a lo largo del tiempo. Hay fuertes evidencias de que la calidad de la infraestructura tiene rol importante en el proceso del desarrollo de las condiciones socioeconómicas. Por ejemplo: es improbable que el impacto social y económico de la implementación de una carretera de un solo carril, sea idéntico al de una carretera con cinco carriles, aunque tengan ambas la misma extensión.

Más allá de los factores económicos, la infraestructura tiene implicaciones importantes en términos del desarrollo social, ya que determina de forma directa el acceso de la población a servicios básicos y asegura una mayor defensa contra desastres, naturales o provocados por el humano. De modo indirecto, el aumento de la productividad de los sectores de la economía, la reducción de los costos de transporte y la creación de puestos de trabajo que pueden derivar de una mejor dotación de servicios de infraestructura también pueden conducir a logros sociales importantes. además de facilitar el acceso de los individuos más pobres a oportunidades productivas y aumentar su capital humano por medio del acceso a servicios de educación y salud, la infraestructura cumple rol fundamental en la integración de esos individuos y sus familias a la vida social y económica.

La infraestructura también tiene repercusiones importantes en el medioambiente, ya que condiciona los patrones de consumo energético de una economía, la generación de desechos y efluentes, y los niveles de emisión de gases de efecto invernadero y otros contaminantes en la atmósfera.

Aunque se reconozca el rol clave de la infraestructura en el desarrollo, se ha documentado un cuadro generalizado de baja inversión en sistemas de energía, transporte, telecomunicaciones, agua y saneamiento: en el conjunto de economías avanzadas y emergentes, el stock de capital público relativo al PIB ha disminuido en unos 15% a lo largo de las últimas tres décadas.

Para el caso de América Latina y el Caribe, la CEPAL ha desarrollado estudios relacionados con el mismo tema en los últimos años. se ha estimado la brecha de infraestructura para la región, calculada como la diferencia entre la inversión en infraestructura y aquella necesaria para satisfacer diversos objetivos de desarrollo. Se encontró que, para el período de 2006 a 2020, sería necesario invertir anualmente en torno al 6,2% del PIB regional para atender a las necesidades de las empresas y de los consumidores finales, al paso que, para alcanzar los niveles de infraestructura per cápita de un conjunto de países del sudeste asiático, las cifras anuales requeridas para igual período ascenderían al 7,9% del PIB. Estudios posteriores han demostrado que los niveles de inversión observados en los países de la región han sido insuficientes con relación a los valores recomendados por los autores, o si se los compara con otras economías en desarrollo.

En el estudio más reciente que ha aplicado la misma metodología de la brecha de infraestructura en América Latina y el Caribe (Sánchez y otros, 2017). Las estimaciones actualizadas para la región

3 Caso práctico 1

Antes de adentrarnos en nuestro problema vamos a conocer un poco la situación actual de las infraestructuras criticas de la base industrial de defensa del ejercito argentino. El Ministerio de Defensa de la Nación Argentina

define las IC de la BID como "aquellos activos o sistemas físicos o virtuales que son esenciales para la producción, adquisición, almacenamiento, distribución y utilización de los recursos materiales y servicios necesarios para la defensa nacional". Estas IC se caracterizan por:

- Su criticidad: Son indispensables para el funcionamiento de la BID y la capacidad de defensa del país.
- Su vulnerabilidad: Son susceptibles a ataques o eventos disruptivos que podrían afectar su funcionamiento.
- Su interdependencia: Están interconectadas con otras IC, lo que amplifica el impacto de su afectación.

3.1 Normativas que Rigen las IC y las INEXTGEN

En Argentina, existen diversas normativas que regulan las IC y las INEXTGEN (infraestructuras críticas de nueva generación), incluyendo:

- Ley Nacional de Seguridad Cibernética (N° 27.341): Establece un marco legal para la protección de las IC frente a ciberataques.
- Decreto N° 1000/2018: Aprueba la Estrategia Nacional de Ciberseguridad, que define las IC y establece lineamientos para su protección.
- Resolución N° 115/2020: Establece los requisitos mínimos de seguridad para las IC.
- Lineamientos de la Organización de Estados Americanos (OEA) para la Protección de Infraestructuras Críticas: Proporcionan recomendaciones para la identificación, evaluación, protección y recuperación de las IC.

3.2 Análisis de las IC de la BID en el Contexto Regional e Internacional

Las IC de la BID del Ejército Argentino deben considerarse en el contexto regional e internacional, donde existen diversas iniciativas y organizaciones que trabajan en la protección de las IC. Algunas de estas iniciativas son:

- El Comité Interamericano contra el Terrorismo (CICTE) de la OEA: Promueve la cooperación entre los países miembros para la protección de las IC.
- El Centro Interamericano de Defensa (CID): Desarrolla estudios e investigaciones sobre las IC y la ciberdefensa.
- La Organización del Tratado del Atlántico Norte (OTAN): Tiene un programa específico para la protección de las IC.

3.3 ¿Qué ocurriría si hay un ataque terrorista a Infraestructuras Críticas argentinas?

El Ejército Argentino, como parte de las Fuerzas Armadas, tiene la responsabilidad de contribuir a la defensa nacional y la seguridad interior del país. En caso de un ataque terrorista a infraestructuras críticas, el Ejército podría actuar de diversas maneras, de acuerdo con las circunstancias específicas del ataque:

- Protección de las infraestructuras: El Ejército podría desplegar tropas para proteger las infraestructuras críticas y evitar nuevos ataques.
- Restauración de servicios: El Ejército podría colaborar con otras entidades para restaurar los servicios afectados por el ataque.
- Búsqueda y captura de los responsables: El Ejército podría participar en la búsqueda y captura de los responsables del ataque.
- Mantenimiento del orden público: El Ejército podría colaborar con las fuerzas de seguridad para mantener el orden público y evitar disturbios sociales.
- Cooperación internacional: El Ejército podría solicitar y/o brindar asistencia a otros países en la investigación y persecución de los responsables del ataque.

Es importante destacar que la respuesta del Ejército Argentino se llevaría a cabo en coordinación con las autoridades civiles y de acuerdo con las leyes vigentes. La decisión de utilizar las Fuerzas Armadas en caso de un ataque terrorista sería tomada por las autoridades competentes, teniendo en cuenta la gravedad de la situación y la necesidad de proteger la seguridad nacional.

Además de la respuesta militar, un ataque terrorista requeriría una respuesta integral que involucraría a diferentes sectores del gobierno, incluyendo organismos de inteligencia (para identificar y prevenir futuros

ataques), fuerzas de seguridad (para investigar el ataque y capturar a los responsables), entidades de emergencia (para atender a las víctimas y restaurar los servicios afectados), organismos gubernamentales (para coordinar la respuesta y tomar medidas para mitigar el impacto del ataque) y por ultimo el sector privado (para colaborar en la restauración de los servicios y la recuperación económica).

3.4 Conclusión

La protección de las IC de la BID del Ejército Argentino es un desafío complejo que requiere un enfoque integral y multisectorial. Es necesario fortalecer el marco legal y regulatorio, desarrollar capacidades de gestión de riesgos, implementar medidas de protección física y cibernética, y fomentar la cooperación internacional. La comprensión de las definiciones, características y normativas que rigen las IC y las INEXTGEN en diversos sectores, tanto a nivel nacional como regional e internacional, es fundamental para diseñar e implementar estrategias efectivas de protección.

4 Caso práctico 2

4.1 Situación de Problema

El Puerto de Buenos Aires es una de las infraestructuras críticas más importantes de Argentina, tanto por su volumen de actividad como por su estratégica ubicación. En los últimos años, se ha incrementado la importación de gas natural licuado (GNL) en barcos metaneros, lo que ha generado preocupación por la posibilidad de que estos buques sean objetivos de ataques terroristas.

4.2 Hipótesis

Existen diversos grupos terroristas con la capacidad y la motivación para atacar objetivos como el Puerto de Buenos Aires y los barcos metaneros. Esta preocupacion surge debido a que a partir de la informacion recolectada se sabe que el promedio por barco es de 70 personas de origen asiatico o arabicos y gracias a la importacion de gas licuado por barcos que deben llegar hasta el canal de Emilio Mitre para depositar el gas. En caso de no seguir el camino correcto el barco terminaria en el canal Norte llegando a Purto Nuevo, este barco llegaria a una ciudad de Puerto Madero. Si se considera que la tripulación tiene intenciones de hacer un ataque terrorista, solo se requiere de un mal control de las coniciones de gas para que explote o ayuda de un dron que uede estallar contra el barco en el momento que se encuentre en la costa. El daño que ocasionaria una explosion como esta constaria de 7 kilometros a la redonda tomando desde la costa hasta el teatro Colón.

Un ataque de este tipo tendría graves consecuencias, incluyendo:

- Pérdidas de vidas humanas y daños a la propiedad.
- Interrupción del suministro de gas natural, lo que podría provocar una crisis energética.
- Daños a la economía nacional y la imagen internacional del país.

4.3 Tesis

Medidas para prevenir un ataque terrorista en el Puerto de Buenos Aires y proteger los barcos metaneros, con énfasis en la infraestructura crítica.

1. Protección de la infraestructura crítica:

1.1. Tanques de almacenamiento de gas:

Ubicación estratégica: Reubicar los tanques de almacenamiento de gas a zonas más seguras dentro del puerto, alejados de áreas pobladas y de fácil acceso. Protección física: Implementar barreras físicas robustas alrededor de los tanques, como muros de hormigón armado o cercas de alta seguridad. Sistemas de detección de intrusiones: Instalar sistemas de detección de intrusiones para alertar al personal de seguridad en caso de intentos de acceso no autorizado a los tanques. Sistemas de extinción de incendios: Implementar sistemas de extinción de incendios avanzados y de fácil activación para minimizar los daños en caso de un incendio o explosión.

1.2. Tuberías: Monitoreo y control: Implementar sistemas de monitoreo y control remoto de las tuberías para detectar fugas, manipulaciones o anomalías en el flujo de gas. Protección contra daños: Instalar protecciones

físicas alrededor de las tuberías para evitar daños accidentales o intencionales, como excavaciones o vandalismo. Válvulas de cierre de emergencia: Instalar válvulas de cierre de emergencia en puntos estratégicos de la red de tuberías para aislar secciones en caso de una fuga o un ataque. Planes de mantenimiento preventivo: Implementar planes de mantenimiento preventivo para detectar y corregir posibles debilidades en las tuberías antes de que ocurran fallas.

1.3. Sistemas de control: Ciberseguridad: Fortalecer la seguridad cibernética de los sistemas de control de la infraestructura crítica, implementando medidas como autenticación multifactor, encriptación de datos y segmentación de redes. Protección contra ataques cibernéticos: Implementar sistemas de detección de intrusiones y de prevención de intrusiones para proteger los sistemas de control contra ataques cibernéticos. Copia de seguridad y recuperación de desastres: Implementar planes de copia de seguridad y recuperación de desastres para garantizar la continuidad operativa en caso de un ataque cibernético o una falla del sistema. Capacitación del personal: Capacitar al personal responsable de la operación y mantenimiento de los sistemas de control en materia de ciberseguridad y protección contra ataques cibernéticos.

2. Integración de la seguridad de la infraestructura crítica en los planes de prevención: Evaluación de riesgos: Realizar evaluaciones de riesgos específicas para la infraestructura crítica del puerto, considerando las amenazas potenciales, las vulnerabilidades y las posibles consecuencias de un ataque. Desarrollo de planes de seguridad: Desarrollar planes de seguridad específicos para la infraestructura crítica, detallando las medidas de prevención, detección, respuesta y recuperación en caso de un ataque. Integración con los planes generales de seguridad: Integrar los planes de seguridad de la infraestructura crítica en los planes generales de seguridad del puerto, asegurando una respuesta coordinada y efectiva en caso de un ataque. Ejercicio y entrenamiento: Realizar ejercicios y simulacros de forma regular para probar los planes de seguridad de la infraestructura crítica y entrenar al personal en su implementación.

3. Tecnologías avanzadas para la protección de la infraestructura crítica: Sensores y detectores: Implementar sensores y detectores específicos para la infraestructura crítica, como sensores de gas, detectores de fugas, sensores de vibración y sistemas de detección de intrusiones. Monitoreo remoto y análisis de datos: Implementar sistemas de monitoreo remoto y análisis de datos para recopilar y analizar información en tiempo real sobre el estado de la infraestructura crítica, permitiendo identificar anomalías y detectar posibles amenazas. Sistemas de alerta temprana: Implementar sistemas de alerta temprana para notificar al personal de seguridad y a las autoridades en caso de detectar anomalías o posibles amenazas en la infraestructura crítica. Tecnologías de inteligencia artificial: Explorar el uso de tecnologías de inteligencia artificial para analizar datos, identificar patrones de comportamiento sospechoso y predecir posibles ataques a la infraestructura crítica.

Es importante destacar que la selección e implementación de las medidas de protección de la infraestructura crítica debe realizarse de manera personalizada, considerando las características específicas del puerto, las amenazas potenciales y los recursos disponibles.

La protección de la infraestructura crítica es un componente esencial de la estrategia general de prevención de ataques terroristas en el Puerto de Buenos Aires. Al implementar medidas efectivas para proteger los tanques de almacenamiento de gas, las tuberías y los sistemas de control, se puede reducir significativamente la vulnerabilidad del puerto y minimizar las consecuencias de un posible ataque.

4.4 Conclusión

La posibilidad de un ataque terrorista en el Puerto de Buenos Aires representa una amenaza significativa para la seguridad nacional, la economía y la imagen del país. Es necesario adoptar un enfoque integral para prevenir este tipo de ataques, que incluya medidas de seguridad física, el uso de tecnologías avanzadas, la mejora de la coordinación y la inteligencia, y la cooperación internacional.

La protección de la infraestructura crítica es un elemento fundamental de este enfoque. Los tanques de almacenamiento de gas, las tuberías y los sistemas de control son objetivos potenciales para los terroristas, y su vulnerabilidad podría tener consecuencias devastadoras. Es necesario implementar medidas específicas para proteger esta infraestructura, como barreras físicas, sistemas de detección de intrusiones, sistemas de extinción de incendios y planes de mantenimiento preventivo.

Las tecnologías avanzadas también juegan un papel importante en la prevención de ataques terroristas. Sensores y detectores, sistemas de monitoreo remoto, análisis de datos, sistemas de alerta temprana e

inteligencia artificial pueden ser herramientas valiosas para identificar anomalías, detectar amenazas y prevenir ataques antes de que ocurran.

La coordinación y la inteligencia son esenciales para una respuesta efectiva a los ataques terroristas. Es necesario establecer canales de comunicación fluidos entre las fuerzas de seguridad, las agencias de inteligencia, las autoridades portuarias y otras entidades relevantes. Se debe compartir información de manera oportuna y se deben desarrollar planes de respuesta coordinados para minimizar los daños y salvar vidas.

La cooperación internacional es otro componente clave de la estrategia de prevención. Es necesario colaborar con países vecinos y organizaciones internacionales para compartir información de inteligencia, realizar operaciones conjuntas de seguridad y desarrollar estrategias de prevención a nivel regional.

En definitiva, la prevención de ataques terroristas en el Puerto de Buenos Aires es una responsabilidad compartida que requiere el compromiso de todos los actores involucrados. El gobierno, las fuerzas de seguridad, el sector privado y la población en general deben trabajar juntos para implementar las medidas necesarias y garantizar la seguridad de este importante puerto.

Es importante destacar que este informe solo presenta un marco general para la prevención de ataques terroristas en el Puerto de Buenos Aires. La implementación de medidas específicas debe realizarse de manera personalizada, considerando las características específicas del puerto, las amenazas potenciales y los recursos disponibles.