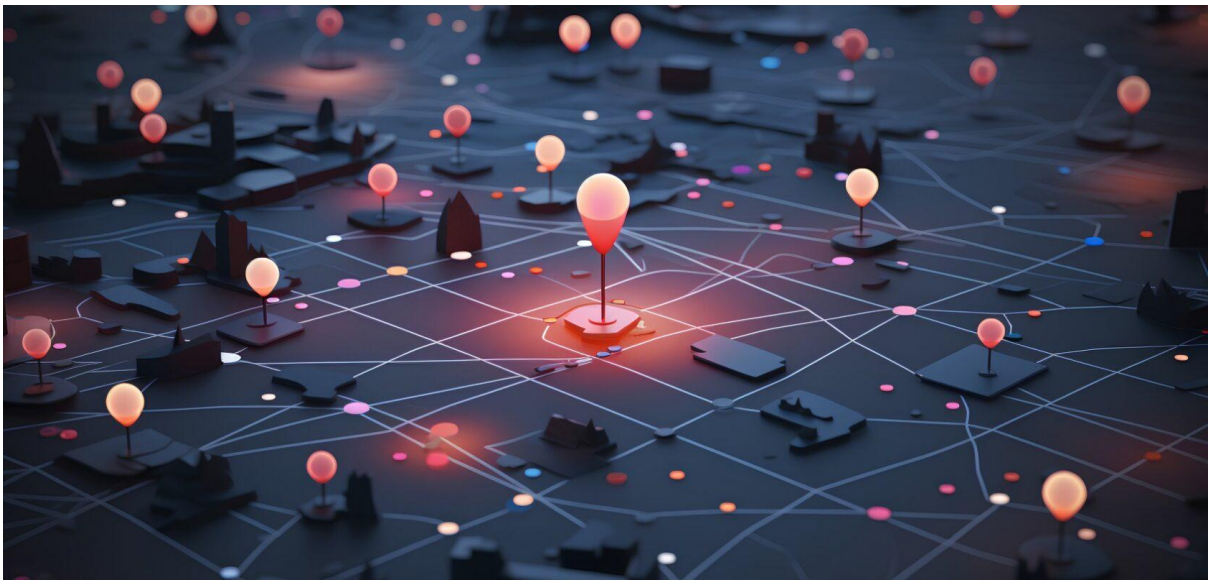
Instituciones como infraestructura crítica: una dimensión olvidada de la resiliencia estratégica en el Cono Sur



Fuente: BILAT.

I. Executive Summary: la estabilidad institucional como infraestructura crítica

Cuando en el Cono Sur se habla de infraestructura crítica, la conversación suele girar en torno a puertos, redes eléctricas, telecomunicaciones, agua potable y transporte. Esta aproximación, aunque necesaria, es incompleta. Existe una categoría de infraestructura igualmente decisiva que permanece, en gran medida, fuera del radar de la planificación estratégica regional: las instituciones del Estado.

Una Cancillería, una autoridad sanitaria, un banco central, un sistema electoral o las Fuerzas Armadas son nodos que permiten que la sociedad funcione y que el Estado ejerza su voluntad colectiva. Al igual que una central eléctrica o un puerto estratégico, estas instituciones pueden ser atacadas, degradadas y neutralizadas, no necesariamente

mediante acción directa o violencia convencional, sino a través de la erosión deliberada de su legitimidad y de la confianza ciudadana en ellas.

Esta es la tesis central del presente análisis: la estabilidad institucional debe ser reconocida y gestionada como infraestructura crítica del Estado. Bajo esa premisa, las campañas de desinformación, la guerra híbrida y la penetración estratégica no son fenómenos exclusivamente comunicacionales o tecnológicos: son vectores de ataque contra los cimientos sobre los cuales reposa la capacidad de decisión soberana.

En el Cono Sur, y en Uruguay en particular, este punto sigue pasando por debajo del radar. El presente trabajo busca contribuir a revertir esa situación, a partir del análisis de evidencia empírica regional y global, y de la identificación de las instituciones más expuestas.

II. Marco conceptual: poder, penetración y guerra híbrida

La dimensión estratégica del Cono Sur es sistemáticamente subestimada. Rara vez existe un consenso interno, más allá de palabras vacías y discursos protocolares, respecto a que geoeconómicamente se trata de una región de interés estratégico. Sin embargo, actores de peso como China, Rusia y los Estados Unidos comprenden y buscan capitalizar ese valor para sus propios intereses geoestratégicos, como lo documenta una cantidad creciente de evidencia empírica.

El economista americano-alemán Klaus Knorr distinguió, en 1975, entre poder militar, poder económico y penetración política como modalidades diferenciadas de influencia entre Estados. La penetración política, cuando agentes de un gobierno extranjero obtienen contacto directo con ciudadanos del Estado objetivo, permite ejercer poder desde dentro del país blanco, sin los costos y la visibilidad de un conflicto convencional. Esta es, precisamente, la razón por la cual la guerra híbrida constituye hoy la punta de lanza de la penetración política.

> *El objetivo no es convencer a la población de algo en particular. El objetivo es erosionar la confianza en los mecanismos mediante los cuales una sociedad se asienta. Si una institución funcional deja de ser creíble, deja de ser capaz de coordinar el comportamiento colectivo.*

Esta lógica explica por qué una nación que desee socavar un orden institucional establecido, para desmerecerlo, reducir la influencia de otros actores en la región, establecer un nuevo status quo o crear un orden institucional paralelo, puede recurrir a campañas de guerra

híbrida y desinformación. La ventaja táctica sobre el conflicto convencional es explícita: la dificultad o imposibilidad de identificar directamente al agresor.

2.1. Evidencia global: Ébola, Ucrania y la anatomía del ataque institucional

Europa ha sufrido en los últimos años una oleada de penetración estratégica mediante campañas híbridas, especialmente tras la invasión rusa de Ucrania en 2022. Los objetivos son claros: obtención de información estratégica, paralización de servidores y difusión de narrativas contrarias a gobiernos e instituciones europeas. Los resultados son visibles: el avance electoral de fuerzas con agenda antieuropea en varios países refleja, en parte, el éxito de esas campañas.

En África, el caso del Ébola en la República Democrática del Congo ofrece un ejemplo distinto pero igualmente ilustrativo. Durante los brotes de 2014 y 2018–2019, la desinformación sobre los mecanismos de la ayuda humanitaria internacional, con foco en las Naciones Unidas, fue instrumentalizada para generar desconfianza y socavar la respuesta sanitaria. Conflictos armados y tensiones preexistentes fueron amplificados por narrativas falsas, comprometiendo gravemente la contención de los brotes. El daño no fue sobre la capacidad técnica de los organismos, sino sobre su legitimidad percibida.

La lectura estratégica de ambos casos es la misma: la variable crítica no es la capacidad real de la institución, sino la percepción social de su legitimidad y funcionalidad. Una institución puede seguir funcionando técnicamente mientras es vaciada de autoridad social. Ese es el objetivo.

2.2. Actores y vectores: HispanTV y la desinformación de Estado en el Cono Sur

Solo a modo de ejemplo, en Iberoamérica, uno de los vectores más documentados de penetración informacional es HispanTV, el canal de noticias en español operado por la Radiodifusora de la República Islámica de Irán (IRIB). Fundado en 2012, el canal fue sancionado por los Estados Unidos en 2013 y 2022 por su papel en la difusión de desinformación y por ser cómplice de violaciones a los derechos humanos. En 2020, YouTube lo prohibió definitivamente de su plataforma. Sin embargo, HispanTV continúa

operando a través de cable, transmisión satelital, redes sociales y su propia plataforma digital, alcanzando audiencias en toda la región.

Un informe de la Liga Antidifamación (ADL) de febrero de 2026, que analizó la programación del canal entre agosto de 2024 y diciembre de 2025, concluye que HispanTV ha intensificado sus esfuerzos de desinformación, combinando narrativas antisemitas, revisionismo histórico y conspiracionismo, con el objetivo de influir en el debate público en América Latina. En el contexto del Cono Sur, el canal opera como instrumento de poder blando iraní, articulado con alianzas ideológicas locales, erosionando narrativas pro-occidental y sembrando desconfianza en las instituciones regionales e internacionales.

La estrategia no es nueva. Los mensajes de HispanTV son amplificados por redes sociales y llegan a diferentes grupos de la sociedad, cumpliendo una función de saturación informacional: no se busca que la audiencia crea una narrativa específica, sino que deje de confiar en cualquier fuente verificada. Esa es la condición previa para vaciar de autoridad a las instituciones.

2.3. La dimensión electoral: desinformación como arma de erosión democrática

Los sistemas electorales son, en este marco, infraestructura institucional de primer orden. Su debilitamiento, real o percibido, afecta directamente la capacidad del Estado de generar autoridad legítima. En el Cono Sur, los procesos electorales de 2023 y 2024 registraron patrones de desinformación sistemática documentados por organizaciones especializadas como Chequeado (Argentina) y el Observatorio Complutense de Desinformación (España).

En Argentina, durante las elecciones presidenciales de octubre de 2023, circularon narrativas falsas sobre fraude masivo, construidas a partir de pequeñas irregularidades presentadas como evidencia de manipulación sistémica. El mismo patrón se reprodujo en Paraguay, Ecuador, México y otros países de la región: una irregularidad marginal —una máquina de votación que funciona mal, una tachadura en un documento oficial— transformada, mediante redes sociales y canales de amplificación, en “evidencia” de fraude organizado.

En Uruguay, el mismo informe del Observatorio Complutense analizó los incidentes de desinformación durante las elecciones de octubre y noviembre de 2024. El país presenta niveles relativamente bajos de desinformación electoral en comparación con otros de la región, lo que respalda la hipótesis de que su estabilidad democrática actúa como factor

mitigante. Sin embargo, esa misma estabilidad puede generar una falsa sensación de invulnerabilidad. Las narrativas detectadas siguen los patrones regionales, y la brecha de percepción respecto a la confianza en las instituciones no es inmune a la degradación sostenida.

2.4. La dimensión cibernética: Uruguay como caso de estudio

La exposición de Uruguay a la presión híbrida tiene una expresión concreta y cuantificable en su infraestructura digital. En 2025, según el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTUY), los ataques a organismos públicos y entidades sensibles superaron en once meses la suma de los cinco años anteriores (equivalente a un nuevo incidente cada trece minutos.) La tendencia se aceleró en 2026: en el primer trimestre los ciberataques aumentaron un 199% respecto al mismo período anterior, con blancos que incluyen infraestructura crítica convencional como el Puerto de Montevideo, el Aeropuerto Internacional de Carrasco, la Represa de Salto Grande y el Data Center de Antel.

Los incidentes de 2025 ilustran con precisión la dimensión institucional del problema. En octubre, el grupo internacional *crypto24* ejecutó el ataque descrito por los analistas como el más grave registrado en Uruguay hasta la fecha: 700 GB de expedientes reservados del Banco Hipotecario del Uruguay, incluyendo litigios judiciales con grandes grupos empresariales y propuestas de conciliación con valor estratégico. La Agencia de Gobierno Electrónico (AGESIC), organismo del que depende la propia política digital del Estado, fue también víctima de ataques durante el año. El sistema GURI de la ANEP, que gestiona la información escolar de primaria, sufrió un incidente que obligó a varias escuelas a operar temporalmente en papel. Ceibal, la Fiscalía y Sucive completaron la lista de blancos institucionales de alto impacto simbólico.

Uno de los desarrollos más preocupantes es la profesionalización del ecosistema atacante. El grupo *LaPampaLeaks* evolucionó de actor hacktivista filtrador a proveedor de servicios de ciberinteligencia comercial, desarrollando *PampaBot:* una herramienta accesible vía Telegram que integra datos robados de múltiples organismos estatales uruguayos y los pone a disposición de terceros a cambio de pago. Esta mutación, del hacktivismo al cibercrimen como servicio, implica que la información institucional comprometida ya no solo se filtra: se comercializa y se reutiliza de forma sostenida.

El comandante de la Unidad de Ciberdefensa del Ejército, coronel Jorge Rahi, fue explícito durante el quinto aniversario de la división en abril de 2026: “El ciberespacio es un dominio de operaciones tan real y determinante como el terrestre, el aéreo, el marítimo o el espacial.”

Cada filtración pública de datos ciudadanos, cada paralización de un servicio estatal, cada operación con mensaje político, como la publicación de la cédula y el teléfono del presidente de Uruguay Yamndú Orsi en la web de DINACI, contribuye a degradar la confianza de la población en la capacidad del Estado de protegerla. Desde una perspectiva de guerra híbrida, eso no es un daño colateral: es el objetivo.

III. Conclusiones y recomendaciones

La convergencia de los fenómenos analizados, desinformación estratégica, manipulación electoral, operaciones cibernéticas y penetración política, apunta a una amenaza común: el debilitamiento de la infraestructura institucional del Estado. No como destrucción física, sino como vaciamiento funcional. Una Cancillería desacreditada no puede conducir política exterior. Un sistema electoral cuestionado no puede generar autoridad legítima. Unas Fuerzas Armadas o Policía asociadas a narrativas de corrupción no pueden garantizar el orden público.

La pregunta que debiera orientar la planificación estratégica en el Cono Sur es precisa: ¿qué instituciones serían más vulnerables si un actor externo quisiera reducir la capacidad de decisión soberana del país? Esa pregunta no tiene hoy, en ninguno de los países de la región, una respuesta sistemática institucionalizada.

A partir del análisis precedente, se formulan las siguientes recomendaciones:

3.1 Ampliar el concepto nacional de infraestructura crítica

Los marcos legales y estratégicos de la región, incluyendo el Decreto 371/020 en Uruguay, deben incorporar explícitamente la dimensión institucional como infraestructura crítica. Esto implica identificar cuáles instituciones son nodos críticos para la capacidad de decisión estatal, mapear sus vulnerabilidades de legitimidad y diseñar planes de resiliencia equivalentes a los que existen para infraestructura física.

3.2 Desarrollar capacidad de detección y respuesta ante operaciones de influencia

La detección de ataques a infraestructura física está relativamente institucionalizada. La detección de operaciones de influencia dirigidas contra instituciones no lo está. Es necesario desarrollar capacidad estatal: en inteligencia, comunicaciones estratégicas y defensa pública, para identificar y responder a campañas de desinformación que tengan

como objetivo la erosión institucional. Esto requiere articulación entre las áreas de defensa, inteligencia, y comunicación gubernamental.

3.3 Fortalecer la resiliencia cibernética del Estado

La tendencia de crecimiento exponencial de los incidentes cibernéticos en Uruguay (triplicados entre 2023 y 2024) exige una respuesta que trascienda la reacción incidental. Es necesario un enfoque de resiliencia estructural: redundancia de sistemas críticos, capacitación sistemática del personal estatal, y coordinación entre organismos públicos y el sector privado en la gestión de incidentes con potencial de impacto institucional.

3.4 Construir narrativa estatal proactiva

La desinformación ocupa vacíos. En ausencia de comunicación estratégica coherente desde las instituciones, las narrativas hostiles se instalan con menor resistencia. Los Estados del Cono Sur deben desarrollar capacidad de comunicación estratégica institucional que no sea meramente reactiva, sino que genere confianza sostenida en la población. Esto no implica propaganda, sino transparencia, consistencia y presencia comunicacional en los espacios donde las narrativas alternativas operan.

3.5 Avanzar en coordinación regional

Dado que los actores que operan estas campañas son extrarregionales y no respetan fronteras, la respuesta puramente nacional tiene límites estructurales. Uruguay, Argentina, Brasil, Chile y Paraguay comparten exposición a los mismos vectores de amenaza. El desarrollo de mecanismos regionales de intercambio de inteligencia sobre operaciones de influencia, y de marcos comunes para la protección de la infraestructura institucional, constituye una deuda estratégica de la región.

Referencias bibliográficas

[1] Knorr, Klaus. ***The Power of Nations:*** The Political Economy of International Relations. Basic Books, 1975.

[2] Nehring, Christopher. ***Bioweapons, Big Pharma and Simple Remedies: The Playbook of Health Disinformation and the Ebola Outbreak in the DRC and Uganda.*** KAS Media África, 2026.

[3]Anti-Defamation League (ADL). ***HispanTV: El medio de comunicación del régimen iraní.*** Informe febrero 2026.

[4] CERTUY / AGESIC. ***Datos de incidentes de ciberseguridad 2025–2026.*** Citados en El Observador, Montevideo, enero 2026; y Semanario Búsqueda, abril 2026.

[5] Observatorio Complutense de Desinformación. I***nforme de desinformación elecciones presidenciales Uruguay 2024.*** Dir-Politics, 2025.

[6] Chequeado. ***Desinformación electoral: qué narrativas circulan en América Latina y cómo contrarrestarlas.*** Diciembre de 2024.

Autores
Coronel Magister Pablo Caubarrere & Nahuel González Frugoni

Información bibliográfica
Cnel. (Mag.) Pablo Caubarrere & Nahuel González Frugoni, »Instituciones como infraestructura crítica: una dimensión olvidada de la resiliencia estratégica en el Cono Sur«. BILAT Junio 2026.

Contacto
BILAT
bilat.org
info@bilat.org