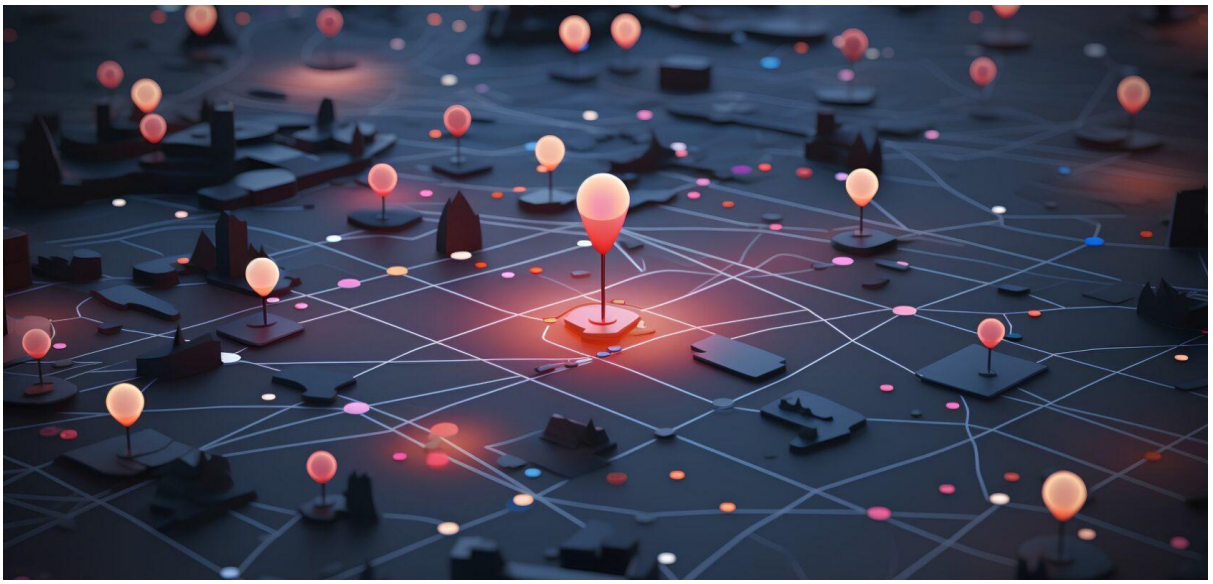
Institutionen als kritische Infrastruktur: Eine vernachlässigte Dimension der strategischen Resilienz im Cono Sur



Quelle: BILAT.

I. Executive Summary: Institutionelle Stabilität als kritische Infrastruktur

Wenn im Cono Sur von kritischer Infrastruktur die Rede ist, dreht sich das Gespräch meist um Häfen, Stromnetze, Telekommunikation, Trinkwasserversorgung und Verkehr. Dieser Ansatz ist zwar notwendig, aber unvollständig. Es gibt eine ebenso entscheidende Kategorie von Infrastruktur, die weitgehend außerhalb des Blickfeldes der regionalen strategischen Planung bleibt: die staatlichen Institutionen.

Ein Außenministerium, eine Gesundheitsbehörde, eine Zentralbank, ein Wahlsystem oder die Streitkräfte sind Knotenpunkte, die das Funktionieren der Gesellschaft ermöglichen und es dem Staat gestatten, seinen kollektiven Willen durchzusetzen. Genau wie ein Kraftwerk oder

ein strategischer Hafen können diese Institutionen angegriffen, geschwächt und neutralisiert werden – nicht unbedingt durch direkte Aktionen oder konventionelle Gewalt, sondern durch die gezielte Untergrabung ihrer Legitimität und des Vertrauens der Bürger in sie.

Dies ist die zentrale These der vorliegenden Analyse: Institutionelle Stabilität muss als kritische staatliche Infrastruktur anerkannt und entsprechend behandelt werden. Unter dieser Prämisse sind Desinformationskampagnen, hybrider Krieg und strategische Unterwanderung keine rein kommunikativen oder technologischen Phänomene: Sie sind Angriffsvektoren, die auf die Grundlagen abzielen, auf denen die souveräne Entscheidungsfähigkeit beruht.

Im Cono Sur, und insbesondere in Uruguay, wird dieses Thema nach wie vor kaum beachtet. Die vorliegende Arbeit soll dazu beitragen, diese Situation zu ändern, indem sie regionale und globale empirische Daten analysiert und die am stärksten betroffenen Institutionen identifiziert.

II. Konzeptioneller Rahmen: Macht, Durchdringung und hybrider Krieg

Die strategische Bedeutung des Cono Sur wird systematisch unterschätzt. Es gibt selten einen internen Konsens – abgesehen von leeren Phrasen und protokollarischen Reden –, dass es sich geoökonomisch gesehen um eine Region von strategischem Interesse handelt. Dennoch erkennen wichtige Akteure wie China, Russland und die Vereinigten Staaten diesen Wert und versuchen, ihn für ihre eigenen geostrategischen Interessen zu nutzen, wie eine wachsende Zahl empirischer Belege zeigt.

Der deutsch amerikanische Ökonom Klaus Knorr identifizierte unterschiedliche Formen der Einflussnahme zwischen Staaten und unterschied 1975 zwischen militärischer Macht, wirtschaftlicher Macht und politischer Durchdringung. Politische Infiltration bei den Akteuren einer ausländischen Regierung direkten Kontakt zu Bürgern des Zielstaates herstellen – ermöglicht es, Macht aus dem Inneren des Ziellandes heraus auszuüben, ohne Kosten oder Visibilität eines konventionellen Konflikts. Genau das ist der Grund, warum der Hybride Krieg heute die Speerspitze der politischen Durchdringung darstellt.

> *Das Ziel besteht nicht darin, die Bevölkerung von etwas Bestimmtem zu überzeugen. Das Ziel ist es, das Vertrauen in die Mechanismen zu untergraben, auf denen eine Gesellschaft beruht. Wenn eine funktionierende Institution ihre*

> *Glaubwürdigkeit verliert, ist sie nicht mehr in der Lage, das kollektive Verhalten zu koordinieren.*

Diese Logik erklärt, warum eine Nation, die eine etablierte institutionelle Ordnung untergraben will – um sie zu diskreditieren, den Einfluss anderer Akteure in der Region zu schwächen, einen neuen Status quo zu etablieren oder eine parallele institutionelle Ordnung zu schaffen –, auf hybride Kriegsführung und Desinformationskampagnen zurückgreifen kann. Der taktische Vorteil gegenüber einem konventionellen Konflikt ist eindeutig: Es ist schwierig bis nahezu unmöglich, den Angreifer direkt zu identifizieren.

2.1 Globale Evidenz: Ebola, die Ukraine und die Struktur des Angriffs auf die Institutionen

Europa war in den letzten Jahren einer Welle strategischer Durchdringung durch hybride Kampagnen ausgesetzt, insbesondere nach dem russischen Einmarsch in die Ukraine im Jahr 2022. Die Ziele sind klar: Beschaffung strategischer Informationen, Lähmung von Servern und Verbreitung von Narrativen, die sich gegen europäische Regierungen und Institutionen richten. Die Ergebnisse sind sichtbar: Der Wahlerfolg von Kräften mit antieuropäischer Agenda in mehreren Ländern spiegelt zum Teil den Erfolg dieser Kampagnen wider.

In Afrika bietet der Ebola-Ausbruch in der Demokratischen Republik Kongo ein anderes, aber ebenso anschauliches Beispiel. Während der Ausbrüche in den Jahren 2014 sowie 2018–2019 wurden Falschinformationen über die Mechanismen der internationalen humanitären Hilfe – mit Schwerpunkt auf den Vereinten Nationen – instrumentalisiert, um Misstrauen zu schüren und die Maßnahmen im Gesundheitswesen zu untergraben. Bestehende bewaffnete Konflikte und Spannungen wurden durch Falschmeldungen noch verschärft, was die Eindämmung der Ausbrüche erheblich beeinträchtigte. Der Schaden betraf nicht die fachlichen Fähigkeiten der Behörden, sondern ihre wahrgenommene Legitimität.

Die strategische Interpretation beider Fälle ist dieselbe: Die entscheidende Variable ist nicht die tatsächliche Leistungsfähigkeit der Institution, sondern die gesellschaftliche Wahrnehmung ihrer Legitimität und Funktionsfähigkeit. Eine Institution kann technisch gesehen weiter funktionieren, während sie ihrer gesellschaftlichen Autorität beraubt wird. Genau das ist das Ziel.

2.2 Akteure und Einflussfaktoren: HispanTV und staatliche Desinformation im Cono Sur

Um ein Beispiel zu geben: In Lateinamerika ist *HispanTV*, der spanischsprachige Nachrichtensender der Rundfunkgesellschaft der Islamischen Republik Iran (IRIB) und einer der am besten dokumentierten Kanäle für Informationsmanipulation. Der 2012 gegründete Sender wurde 2013 und 2022 von den Vereinigten Staaten wegen seiner Rolle bei der Verbreitung von Desinformation und wegen Beihilfe zu Menschenrechtsverletzungen sanktioniert. Im Jahr 2020 hat YouTube den Sender endgültig von seiner Plattform verbannt. HispanTV ist jedoch weiterhin über Kabel, Satellitenübertragung, soziale Medien und seine eigene digitale Plattform aktiv und erreicht Zuschauer in der gesamten Region.

Ein Bericht der *Anti-Defamation League* (ADL) vom Februar 2026, in dem das Programm des Senders zwischen August 2024 und Dezember 2025 analysiert wurde, kommt zu dem Schluss, dass *HispanTV* seine Bemühungen im Bereich der Desinformation verstärkt hat, indem es antisemitische Narrative, Geschichtsrevisionismus und Verschwörungstheorien miteinander vermischt, um die öffentliche Debatte in Lateinamerika zu beeinflussen. Im Kontext des Cono Sur fungiert der Sender als Instrument der iranischen *Soft Power*, das mit lokalen ideologischen Bündnissen verzahnt ist, pro-westliche Narrative untergräbt und Misstrauen gegenüber regionalen und internationalen Institutionen sät.

Diese Strategie ist nicht neu. Die Botschaften von *HispanTV* werden über soziale Netzwerke verbreitet und erreichen verschiedene gesellschaftliche Gruppen, wodurch sie eine Funktion der Informationsüberflutung erfüllen: Es geht nicht darum, dass das Publikum einer bestimmten Erzählung glaubt, sondern dass es Vertrauen in verifizierte Quellen verliert. Das ist die Voraussetzung dafür, den Institutionen ihre Autorität zu entziehen.

2.3 Die elektorale Dimension: Desinformation als Waffe zur Zersetzung der Demokratie

Wahlsysteme stellen in diesem Zusammenhang eine institutionelle Infrastruktur von höchster Bedeutung dar. Ihre – tatsächliche oder vermeintliche – Schwächung beeinträchtigt unmittelbar die Fähigkeit des Staates, legitime Autorität zu schaffen. Im Cono Sur zeigten die Wahlprozesse der Jahre 2023 und 2024 Muster systematischer Desinformation, die von spezialisierten Organisationen wie „*Chequeado*“ (Argentinien) und dem *Observatorio Complutense de Desinformación* (Spanien) dokumentiert wurden.

In Argentinien kursierten während der Präsidentschaftswahlen im Oktober 2023 falsche Darstellungen über massiven Wahlbetrug, die auf geringfügigen Unregelmäßigkeiten beruhten, jedoch als Beweis für eine systematische Manipulation dargestellt wurden. Dasselbe Muster wiederholte sich in Paraguay, Ecuador, Mexiko und anderen Ländern der Region: Eine marginale Unregelmäßigkeit – eine fehlerhafte Wahlmaschine, eine Streichung in einem offiziellen Dokument – wurde über soziale Medien und Verbreitungskanäle zu „Beweisen" für organisierten Wahlbetrug hochgespielt.

Auch in Uruguay analysierte der Bericht des *Observatorio Complutense* Fälle von Desinformation während der Wahlen im Oktober und November 2024. Das Land wies im Vergleich zu anderen Ländern der Region ein relativ geringes Ausmaß an Desinformation im Wahlkampf auf, was die Hypothese stützt, dass seine demokratische Stabilität als mildernder Faktor wirkt. Diese Stabilität kann jedoch ein falsches Gefühl der Unverwundbarkeit hervorrufen. Das festgestellte Narrativ folgt den regionalen Mustern, und die Kluft in der Wahrnehmung hinsichtlich des Vertrauens in die Institutionen ist nicht immun gegen einen anhaltenden Verfall.

2.4 Die Cyber-Dimension: Uruguay als Fallstudie

Die hybriden Bedrohungen, denen Uruguay ausgesetzt ist, zeigen sich konkret und messbar in der digitalen Infrastruktur. Im Jahr 2025 überstieg die Zahl der Angriffe auf öffentliche Einrichtungen und sensible Stellen laut dem uruguayischen *Centro Nacional de Respuesta a Incidentes de Seguridad Informática* (CERTuy, dt. Nationales Zentrum für die Reaktion auf IT-Sicherheitsvorfälle) innerhalb von elf Monaten die Summe der vorangegangenen fünf Jahre – was einem neuen Vorfall alle dreizehn Minuten entspricht. Dieser Trend beschleunigte sich im Jahr 2026: Im ersten Quartal stiegen die Cyberangriffe im Vergleich zum Vorjahreszeitraum um 199%, wobei zu den Zielen konventionelle kritische Infrastrukturen wie der Hafen von Montevideo, der internationale Flughafen Carrasco, der Staudamm Salto Grande und das Rechenzentrum des staatseigenen Telekommunikationsunternehmen *Administración Nacional de Telecomunicaciones* (ANTEL) gehörten.

Die Vorfälle des Jahres 2025 verdeutlichen anschaulich die institutionelle Dimension des Problems. Im Oktober führte die internationale Gruppe „*crypto24*" einen Angriff durch, den Analysten als den bislang schwerwiegendsten in Uruguay bezeichneten: 700 GB

vertraulicher Unterlagen der uruguayischen Hypothekenbank *Banco Hipotecario del Uruguay*, darunter Gerichtsverfahren mit großen Unternehmenskonzernen und Vergleichsvorschläge von strategischer Bedeutung. Die *Agencia de Gobierno Electrónico* (AGESIC, dt. Agentur für elektronische Verwaltung) – die für die digitale Politik des Staates zuständige Behörde – wurde im Laufe des Jahres ebenfalls Opfer von Angriffen. Das GURI-System der uruguayischen *Administración Nacional de Educación Pública* (ANEP, dt. Nationale Verwaltung für das öffentliche Bildungswesen), das die Schuldaten der Grundschulen verwaltet, war von einem Vorfall betroffen, der mehrere Schulen dazu zwang, vorübergehend auf Papier umzustellen. Institutionen wie die digitale Bildungsbehörde *Ceibal*, die Generalstaatsanwaltschaft und das zentrale Kfz-Registersystem *Sucive* vervollständigten die Liste der institutionellen Ziele von hoher symbolischer Bedeutung.

Eine der besorgniserregendsten Entwicklungen ist die Professionalisierung des Bedrohungslandschaft. Die Gruppe *LaPampaLeaks* hat sich von einem hacktivistischen Akteur, der Daten veröffentlichte, zu einem Anbieter kommerzieller Cyber-Intelligence-Dienste gewandelt und dabei „*PampaBot*“ entwickelt: ein über Telegram zugängliches Tool, das gestohlene Daten aus zahlreichen staatlichen Stellen Uruguays zusammenführt und diese Dritten gegen Bezahlung zur Verfügung stellt. Die Wandlung vom Hacktivismus zur Cyberkriminalität als Dienstleistung bedeutet, dass kompromittierte institutionelle Informationen nicht mehr nur geleakt werden, sondern kommerzialisiert und nachhaltig wiederverwendet werden.

Der Kommandant der Cyberabwehr-Einheit der Armee, Oberst Jorge Rahi, äußerte sich anlässlich des fünfjährigen Bestehens der Einheit im April 2026 unmissverständlich: „Der Cyberspace ist ein Einsatzgebiet, das ebenso real und entscheidend ist wie der Land-, Luft-, See- oder Weltraum.“ Jedes öffentliche Datenleck, jede Lähmung eines staatlichen Dienstes, jede Operation mit politischer Botschaft – wie die Veröffentlichung der Personalausweisnummer und der Telefonnummer von Präsident Orsi auf der Website der DINACIA – trägt zur Schwächung des Vertrauens der Bevölkerung in die Fähigkeit des Staates bei, sie zu schützen. Aus der Perspektive eines hybriden Krieges ist das kein Kollateralschaden: Es ist das Ziel.

III. Schlussfolgerungen und Empfehlungen

Das Zusammenspiel der untersuchten Phänomene – strategische Desinformation, Wahlmanipulation, Cyberoperationen und politische Unterwanderung – deutet auf eine gemeinsame Bedrohung hin: die Schwächung der institutionellen Infrastruktur des Staates. Nicht im Sinne einer physischen Zerstörung, sondern im Sinne einer funktionalen Aushöhlung. Ein diskreditiertes Außenministerium kann keine Außenpolitik betreiben. Ein in Frage gestelltes Wahlsystem kann keine legitime Autorität schaffen. Streitkräfte oder eine Polizei, die mit Korruptionsvorwürfen in Verbindung gebracht werden, können die öffentliche Ordnung nicht gewährleisten.

Die Frage, die der strategischen Planung im Cono Sur die Richtung weisen sollte, kann präzise formuliert werden: Welche Institutionen wären am anfälligsten, wenn ein externer Akteur die souveräne Entscheidungsfähigkeit des Landes einschränken wollte? Darauf gibt es heute in keinem der Länder der Region eine systematische, institutionalisierte Antwort.

Auf der Grundlage der vorstehenden Analyse werden folgende Empfehlungen ausgesprochen:

3.1 Ausweiten des nationalen Konzepts der kritischen Infrastruktur

Die rechtlichen und strategischen Rahmenbedingungen der Region – darunter das Dekret 371/020 in Uruguay – müssen die institutionelle Dimension ausdrücklich als kritische Infrastruktur einbeziehen. Dies bedeutet, dass ermittelt werden muss, welche Institutionen für die Entscheidungsfähigkeit des Staates von entscheidender Bedeutung sind, dass die Schwachstellen hinsichtlich ihrer Legitimität erfasst werden und dass Resilienzpläne entworfen werden, die denen der physischen Infrastruktur entsprechen.

3.2 Aufbau von Kapazitäten zur Erkennung von und Reaktion auf Einflussnahmen

Das Erkennen von Angriffen auf die physische Infrastruktur ist relativ gut institutionalisiert. Das gilt jedoch nicht für die Erkennung von Einflussnahmen, die sich gegen Institutionen richten. Es ist notwendig, staatliche Kapazitäten – in den Bereichen Nachrichtendienst, strategische Kommunikation und öffentliche Sicherheit – aufzubauen, um Desinformationskampagnen, die auf eine Aushöhlung der Institutionen abzielen, zu erkennen

und darauf zu reagieren. Dies erfordert eine enge Zusammenarbeit zwischen den Bereichen der Verteidigung, des Nachrichtendienstes und der Regierungskommunikation.

3.3 Stärken der Cyberresilienz des Staates

Der Trend des exponentiellen Anstiegs von Cybervorfällen in Uruguay – deren Zahl sich zwischen 2023 und 2024 verdreifacht hat – erfordert eine Antwort, die über eine bloße Reaktion auf einzelne Vorfälle hinausgeht. Es bedarf eines Ansatzes zur strukturellen Resilienz: Redundanz kritischer Systeme, systematische Fortbildung des staatlichen Personals sowie die Koordinierung zwischen öffentlichen Stellen und dem privaten Sektor bezüglich des Managements von Vorfällen mit potenziellen institutionellen Auswirkungen.

3.4 Entwickeln eines proaktiven staatlichen Narrativs

Desinformation füllt Lücken. In Ermangelung einer kohärenten strategischen Kommunikation seitens der Institutionen können sich feindselige Narrative ohne großen Widerstand etablieren. Die Staaten des Cono Sur müssen institutionelle Kapazitäten für strategische Kommunikation aufbauen, die nicht nur reaktiv sind, sondern in der Bevölkerung nachhaltiges Vertrauen schaffen. Dabei geht es nicht um Propaganda, sondern um Transparenz, Konsistenz und eine starke Kommunikationspräsenz in den Bereichen, in denen alternative Narrative verbreitet werden.

3.5 Fortschritte bei der regionalen Zusammenarbeit

Da die Akteure, die diese Kampagnen durchführen, überregional agieren und keine Grenzen kennen, stößt eine rein nationale Reaktion an strukturelle Grenzen. Uruguay, Argentinien, Brasilien, Chile und Paraguay sind denselben Bedrohungsfaktoren ausgesetzt. Das Entwickeln regionaler Mechanismen für den Austausch von Informationen über Einflussnahmen sowie gemeinsamer Rahmenbedingungen für den Schutz der institutionellen Infrastruktur ist eine strategische Aufgabe für die Region.

Literatur

[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.

Autoren
Coronel Magister Pablo Caubarrere & Nahuel González Frugoni

Bibliografische Angaben
Oberst. (Mag.) Pablo Caubarrere & Nahuel González Frugoni, »Institutionen als kritische Infrastruktur: Eine vernachlässigte Dimension der strategischen Resilienz im Cono Sur«. BILAT Juni 2026.

Kontakt
BILAT
bilat.org
info@bilat.org