KONRAD ADENAUER STIFTUNG

The Institute for Strategy & Defense Research

Influencias híbridas en México y Alemania

La combinación de tácticas híbridas como herramienta explosiva: Así deberían protegerse los Estados frente a las amenazas modernas

Policy Brief

Mtro. Ferdinand Gehringer
Mtro. Maximilian Strobel

Abstract

Los conflictos actuales ya no son necesariamente peleados por fuerzas militares; en su lugar, los actores estatales, así como los no estatales del siglo XXI intentan influir en otros Estados y sus sociedades por medio de estrategias flexibles, dinámicas y difusas. Nuestro mundo ha cambiado radicalmente, en gran medida debido a los avances tecnológicos que facilitan la vida cotidiana de las personas, pero al mismo tiempo ofrecen nuevos puntos de acceso y de ataques digitales.

Este informe presenta en qué consisten las tácticas híbridas y cómo se utilizan. Además, se presentan ejemplos concretos de operaciones de influencia híbrida en Alemania y México con el fin de ilustrar las particularidades de estas tácticas y mostrar qué medidas políticas urge adoptar en ambos países para protegerse mejor en el futuro.

Desestabilización mediante ocultación y atribución grave

Las tácticas híbridas son medios en los escenarios de conflicto modernos, que consisten en el uso combinado de diferentes instrumentos. El objetivo del uso de estas tácticas es influir en los asuntos estatales o interestatales, perturbar y desestabilizar las sociedades y/o influir en la opinión pública.[1]

Los actores responsables pueden ser tanto estatales como no estatales. En este contexto, los actores estatales en particular también utilizan a grupos privados y delincuentes para alcanzar sus objetivos y reforzar el encubrimiento de sus acciones. El requisito para ello es que estos actores cuenten con los medios adecuados para poder ejercer una influencia, manipulación o presión encubiertas (Hoffman, 2007). Esto hace que la atribución, la asignación de responsabilidad de una táctica sea mucho más difícil y, a menudo, sólo es posible con un tiempo de retraso.

Los actores actúan por debajo del marco de la confrontación armada. Esto significa que sus acciones no pueden calificarse de ataques militares abiertos (Giannopoulos et al., 2021). En consecuencia, una respuesta (militar) de acuerdo con el derecho de guerra (*ius ad bellum*) queda excluida. El estado de «híbrido» intenta captar la fase entre la paz y la guerra, a menudo también denominada estado de «discordia», por lo que al estado de «híbrido» no le sigue necesariamente el de «guerra» (Hoffman, 2007).

[1] https://www.bmvg.de/de/themen/sicherheitspolitik/hybride-bedrohungen

Explotación diversa de las debilidades sistémicas

El uso de tácticas híbridas pretende debilitar al oponente e influir en su comportamiento. Idealmente, permiten obligar al oponente a comportarse de una determinada manera que sirva a los propios intereses. Puede tratarse de concesiones políticas, ventajas económicas o el debilitamiento de la posición internacional del oponente (Giannopoulos et al., 2021).

Las tácticas híbridas se dirigen a las debilidades sistémicas del oponente. Los actores explotan vulnerabilidades en el ámbito social, económico, político, militar o tecnológico. Existen alrededor de 40 tácticas híbridas diferentes. Las principales tácticas híbridas incluyen los ciberataques y la explotación de las filtraciones de datos, los ataques a infraestructuras críticas, la presión económica, la propaganda selectiva, la desinformación y la migración.

Los ciberataques contra las infraestructuras informáticas permiten robar datos e información, paralizar sistemas o difundir desinformación.

Los ataques digitales o físicos contra las infraestructuras críticas pueden paralizar las operaciones e interrumpir los servicios sociales y estatales básicos. Las infraestructuras críticas incluyen el suministro de energía y agua, el transporte y el tráfico, las tecnologías de la información y las telecomunicaciones.

Las **sanciones comerciales, los embargos u otras medidas económicas** pueden utilizarse para desestabilizar la economía de un país o presionar al gobierno para que haga determinadas concesiones. También las inversiones pueden considerarse una medida híbrida, ya que son un medio de ganar influencia política y hacerse con el control, como las inversiones de China en proyectos de infraestructura en todo el mundo.

La **difusión selectiva de información falsa o manipulada** en los medios de comunicación y las redes sociales pretende influir en la opinión pública y agravar la polarización social.

Provocar, favorecer o apoyar activamente los movimientos **migratorios irregulares** también puede ser utilizado de manera puntual para causar inestabilidad política, económica o social en otro Estado, como demuestra el uso que Rusia hace de la migración como arma política en las fronteras exteriores de la Unión Europea (UE).

Combinación y acumulación como mezcla explosiva

Las tácticas individuales pueden causar enormes daños sociales, económicos y/o políticos. Sin embargo, la mayor amenaza es, sin duda, la combinación y acumulación de diferentes tácticas. Un ejemplo de ello es la combinación de ciberataques con campañas de desinformación para crear inestabilidad política y socavar la confianza en las instituciones democráticas.[2]

[2] https://www.nato.int/cps/en/natohq/topics_156338.htm

Un escenario de este tipo podría ser el siguiente:

1. Ciberataques a la infraestructura electoral

Grupos de hackers, posiblemente apoyados por entidades extranjeras, llevan a cabo ciberataques contra las infraestructuras informáticas que deben garantizar el buen desarrollo de las elecciones. Esto puede incluir la piratería de los registros de votantes, de los sistemas de votación o la paralización de los sitios web de las comisiones electorales.

2. Difusión de desinformación

Paralelamente a los ciberataques, se lanza una campaña de desinformación en las redes sociales y otras plataformas digitales. Esta campaña podría difundir información falsa sobre fraude electoral, resultados electorales manipulados o supuestas brechas de seguridad en la infraestructura electoral.

3. Amplificación a través de noticias falsas y bots de redes sociales

Para amplificar el efecto de la desinformación, se crean y difunden artículos de noticias falsas a través de bots de redes sociales y otras cuentas falsas o no auténticas. Estos bots pueden compartir, dar «me gusta» y comentar contenidos automáticamente para crear la apariencia de un amplio apoyo público o de indignación social.

4. Vídeos e imágenes manipulativos o manipulados

El uso de tecnologías deepfake para crear vídeos e imágenes manipulados o ficticios que muestran a candidatos políticos en situaciones comprometidas o escandalosas. Este contenido también se distribuye principalmente a través de las redes sociales para socavar la confianza del público en determinados políticos.

5. Explotar las tensiones sociales y políticas existentes

Las campañas de desinformación pretenden agravar las tensiones sociales y políticas existentes en el país o los países de destino. En México, por ejemplo, temas como la corrupción estatal, los delitos violentos contra inocentes y el comportamiento de los cárteles de la droga se abordan deliberadamente con contenidos en parte falsificados para alimentar los temores, así como la desconfianza o la ira. En Alemania, tienen un gran potencial de división temas como el tratamiento de la migración y la integración, el debate sobre la inmigración de mano de obra calificada, el apoyo a Ucrania en la guerra de agresión rusa o el apoyo a Israel en el conflicto de Cercano Oriente.

Alemania en el punto de mira de los actores extranjeros

Alemania y México son países con diferentes características políticas, geográficas y socioeconómicas; sin embargo, ambos son igualmente objetivos interesantes para la influencia híbrida por parte de actores externos, aunque con diferentes enfoques e intenciones.

Alemania es un país atractivo para las operaciones de influencia híbrida al ser un actor central de la UE, la mayor economía de Europa, el centro logístico dentro de la alianza de la OTAN y el emplazamiento más importante para las fuerzas estadounidenses fuera de los EE. UU. Aparte de la influencia rusa a través de campañas controladas de desinformación, espionaje e intentos de sabotaje de infraestructuras críticas, China, Turquía e Irán son especialmente activos en Alemania.

El año pasado, las cuentas de correo electrónico del Partido Socialdemócrata (SPD), partido gobernante y también del actual canciller federal, Olaf Scholz, fueron atacadas por unos hackers. En junio de 2023, el SPD anunció que las cuentas de la ejecutiva del partido ya habían sido objeto de un ciberataque en enero de ese año. Esto fue posible gracias a una vulnerabilidad de seguridad de la empresa de software Microsoft que aún se desconocía en el momento del ataque. Es posible también que algunos datos se hayan filtrado.[3]

Pocos meses después, la Unión Cristianodemócrata (CDU), actualmente el mayor partido de la oposición en Alemania sufrió un ciberataque. Supuestamente, en este caso también se filtraron datos, incluidos los del líder del partido y del grupo parlamentario, Friedrich Merz.[4]

El grupo de hackers ruso APT 28, cercano al servicio de inteligencia militar ruso GRU, fue el responsable del ciberataque al SPD en Alemania en abril de 2024.[5] La investigación sobre el ataque a la CDU continúa. También en este caso, las autoridades encargadas de la investigación y la acusación suponen que estuvo involucrado un agente estatal profesional.

Desde el comienzo de la invasión rusa de Ucrania en febrero de 2022, una campaña rusa de desinformación a gran escala está activa en Alemania con la campaña «Doppelgänger». El principal objetivo de la campaña es sembrar la duda sobre los valores democráticos liberales y poner en cuestión los fundamentos del orden democrático liberal mediante la difusión de información deliberadamente falsa y narrativas prorrusas.

[3] https://www.tagesschau.de/inland/innenpolitik/spd-hacker-russland-100.html
[4] https://www.zdf.de/nachrichten/politik/deutschland/cdu-cyber-angriff-merz-100.html
[5] https://www.spiegel.de/politik/deutschland/bundesregierung-ordnet-hackerangriff-der-spd-zentrale-russland-zu

En concreto, la campaña pretende principalmente desacreditar el apoyo alemán a Ucrania. Incluye imitaciones con apariencia engañosa de sitios web alemanes de noticias relevantes, como Spiegel, Süddeutsche Zeitung y BILD. Los sitios web apócrifos difunden noticias falsas, a menudo sobre temas políticos, con el fin de alimentar la incertidumbre y la desconfianza. Los artículos falsos, algunos de los cuales están creados mediante inteligencia artificial generativa (IA), se distribuyen luego a través de las redes sociales (por ejemplo, a través de X, antes Twitter, Facebook, YouTube y TikTok) y otras plataformas en línea con el fin de maximizar su alcance. Otro elemento de la campaña es el uso de una compleja infraestructura técnica que incluye servidores alquilados a empresas europeas. Esta infraestructura permite a los operadores, alojar y distribuir los sitios web, contenidos falsos y ocultar la autoría de estos.[6]

Un ejemplo concreto de desinformación en el marco de la campaña «Doppelgänger» son las afirmaciones de que las armas suministradas a Ucrania acaban en el mercado negro de Alemania.[7] Otro ejemplo son los artículos de noticias falsas que acusan al gobierno alemán de congelar fondos para pensiones y gastos sociales con el fin de financiar el suministro de armas a Ucrania. A pesar de los esfuerzos de las autoridades europeas de investigación y de plataformas como Facebook y Twitter/X por detener la campaña de desinformación, ésta sigue activa. La Oficina Bávara para la Protección de la Constitución ha realizado al menos amplios análisis técnicos y ha podido hacerse una idea significativa del modo de funcionamiento de la campaña.[8]

A finales de 2021, la Agencia Federal de Cartografía y Geodesia (BKG) fue víctima de un grave ciberataque que se atribuye a agentes estatales chinos. El ataque es un impresionante ejemplo de espionaje como forma de influencia híbrida china. Su objetivo era robar datos sensibles e infiltrarse en la red de la BKG, lo que pone de relieve la importancia estratégica de la recopilación de información para China.[9] Por ejemplo, la BKG proporciona geodatos de algunas infraestructuras críticas (empresas de suministro de agua, energía y transporte) en Alemania.[10]

Los atacantes utilizaron redes encubiertas comprometiendo los dispositivos de personas y empresas privadas con el fin de cubrir sus huellas y ocultar el origen del ataque. Este tipo de ciberataques socavan la confianza en las instituciones del Estado y en la ciberseguridad, lo que puede conducir a largo plazo a la desestabilización política y económica. El gobierno alemán ha condenado enérgicamente el ataque y ha convocado al embajador chino, lo que subraya las tensiones diplomáticas que pueden derivarse de este tipo de ciberataques.

[6] https://www.auswaertiges-amt.de/blob/2660362/73bcc0184167b438173e554ba2be2636/technischer-bericht-desinformationskampagne-doppelgaenger-data.pdf

[7] https://correctiv.org/faktencheck/hintergrund/2022/09/30/gefaelschte-regierungsdokumente-und-nachrichtenseiten-russische-desinformationskampagne-nimmt-deutschland-ins-visier-prigoschin/

[8] https://www.verfassungsschutz.bayern.de/ueberuns/medien/pressemitteilungen/desinformationskampagne-doppelgaenger/

[9] https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/07/cyberangriff-bkg.html

[10] https://www.tagesschau.de/inland/innenpolitik/ermittlungen-hackerangriff-bundesamt-kartographie-100.html

México como objetivo y punto de tránsito de la influencia extranjera

México es un actor clave en América Latina; el único vecino al sur de Estados Unidos ya fue un lugar popular para los espías rusos durante la Guerra Fría y sigue siendo una puerta atractiva en la actualidad: se dice que el servicio secreto ruso GRU no tiene más agentes destacados en ningún otro país del mundo.

La influencia directa en el mismo México, como puerta de entrada o puente hacia Estados Unidos, convierten al país en punto de tránsito y objetivo de tácticas híbridas. Rusia y China, en particular, están tratando de ejercer influencia en México y, a través de éste, en los Estados Unidos, también por medio de aliados regionales como Cuba, Venezuela y Nicaragua.[11] También hay sospechas de que grupos delictivos de Rusia y China están vinculados a poderosos grupos de delincuencia organizada de México.[12] [13]

Ya hubo reportes de ciberataques al Instituto Nacional Electoral (INE) y a partidos políticos durante la campaña presidencial de 2018.[14] [15] Se sospechaba que agentes extranjeros intentaban obtener información sensible mediante piratería informática, difundirla y socavar así la confianza de la población en el proceso electoral y en las instituciones estatales implicadas.

Durante el último debate televisivo, el sitio web del partido de la oposición Partido Acción Nacional (PAN) quedó paralizado por un ataque de sobrecarga (el llamado ataque DDoS). Se sospechó entonces que China y Rusia eran los responsables de los ciberataques.

En septiembre de 2022 se publicaron seis terabytes de información robada y altamente sensible de la Secretaría de la Defensa Nacional (Sedena) de México.[16] Un grupo internacional de piratas informáticos llamado «Guacamaya» fue responsable del incidente del mismo nombre, Guacamaya Leaks, que supuso la mayor filtración de datos de la historia del país. Salieron a la luz comunicaciones secretas entre partes del ejército, así como la conocida, pero nunca probada cooperación entre políticos, fuerzas de seguridad, cárteles de la droga y el poder judicial.

El ejército mexicano quedó expuesto ante la evidencia pública de su creciente control sobre el gobierno civil y las infraestructuras, la grave corrupción institucional, los intentos de impedir investigaciones sobre violaciones de derechos humanos y el uso del programa espía Pegasus contra periodistas.[17]

[11] Evan Ellis: Chinese engagement in Latin America | OPEU

[12] China, Mexico, and America's fight against the fentanyl epidemic | Brookings

[13] Hydra Market: the financial nexus that linked Russia to the Mexican cartels | Infobae

[14] En elecciones del 2018, INE soportó el mayor ataque cibernético | El Financiero

[15] Cyber attack on Mexico campaign site triggers election nerves | Reuters

[16] Major Mexican Government Hack Reveals Military Abuse and Spying | The New York Times

[17] Guacamaya Leaks: 5 revelaciones del hackeo masivo que sufrió el ejército de México - BBC News

El hackeo sigue siendo un daño irreparable para el ejército mexicano, tanto a nivel interno como externo, y ha tenido como consecuencia una inversión insuficiente en ciberdefensa y consecuencias políticas.[18]

Las campañas de desinformación también son una herramienta popular de manipulación selectiva en México, especialmente durante las campañas electorales; sin embargo, no está muy claro quién está detrás de la difusión de la desinformación.[19] [20] En el periodo previo a las elecciones presidenciales de 2024, el pueblo mexicano se vio enfrentado a una enorme cantidad de desinformación, sobre todo en las redes sociales. Entre otras cosas, se difamó a la candidata Claudia Sheinbaum por sus raíces judías; se rumoreó que convertiría la basílica más importante del país en un museo o que las circuncisiones serían obligatorias bajo su presidencia.

El año pasado aumentó la difusión selectiva de información falsa sobre la posible candidata de la oposición, Xóchitl Gálvez, según la cual recortaría los programas sociales para los sectores más pobres de la población. El presidente Andrés Manuel López Obrador (AMLO) repetía regularmente esta narrativa en sus conferencias de prensa matutinas, las mañaneras. Un aspecto interesante y diferente a las campañas en Alemania es que el propio presidente es un factor central en la difusión de información falsa con el fin de dividir a la sociedad. Sus acusaciones fueron difundidas en línea por sitios con vínculos estrechos al gobierno, un procedimiento que también es conocido en los Estados Unidos.[21]

Además, en los últimos años, Rusia ha incrementado significativamente sus actividades mediáticas en toda América Latina, a menudo con el objetivo de socavar la reputación de las democracias liberales occidentales en el continente. Canales como Sputnik Mundo y Russia Today (RT en español) son ejemplos notables de esa estrategia claramente visible; las narrativas y opiniones geopolíticas (interpretaciones) del Kremlin se difunden gratuitamente en español a través de la radio, la televisión, internet y la prensa escrita con un revestimiento profesional. Una narrativa común es el retrato de Occidente como intervencionista, mientras que los gobernantes autoritarios como el de Ortega, en Nicaragua, o el de Maduro en Venezuela. se presentan como defensores de la soberanía de sus pueblos - siempre implicando que otros países se arriesgan a ser intervenidos si no permanecen vigilantes. La apertura del panorama mediático en la región y la falta de conocimientos de la población sobre los medios de comunicación son explotadas de esta manera. Como vecino directo de Estados Unidos, México es uno de los principales objetivos de las campañas de desinformación rusas.[22]

Los movimientos migratorios también pueden considerarse una amenaza híbrida en ciertas condiciones, como cuando son facilitados deliberadamente. Por ejemplo, resulta evidente que Nicaragua es un centro abierto para los inmigrantes irregulares a los que se permite entrar libremente desde África, India, Haití o Cuba para dirigirse hacia el norte a través de México.

[18] Mexico's National Cybersecurity Policy: Progress Has Stalled Under AMLO - Carnegie Russia Eurasia Center | carnegieendowment.org

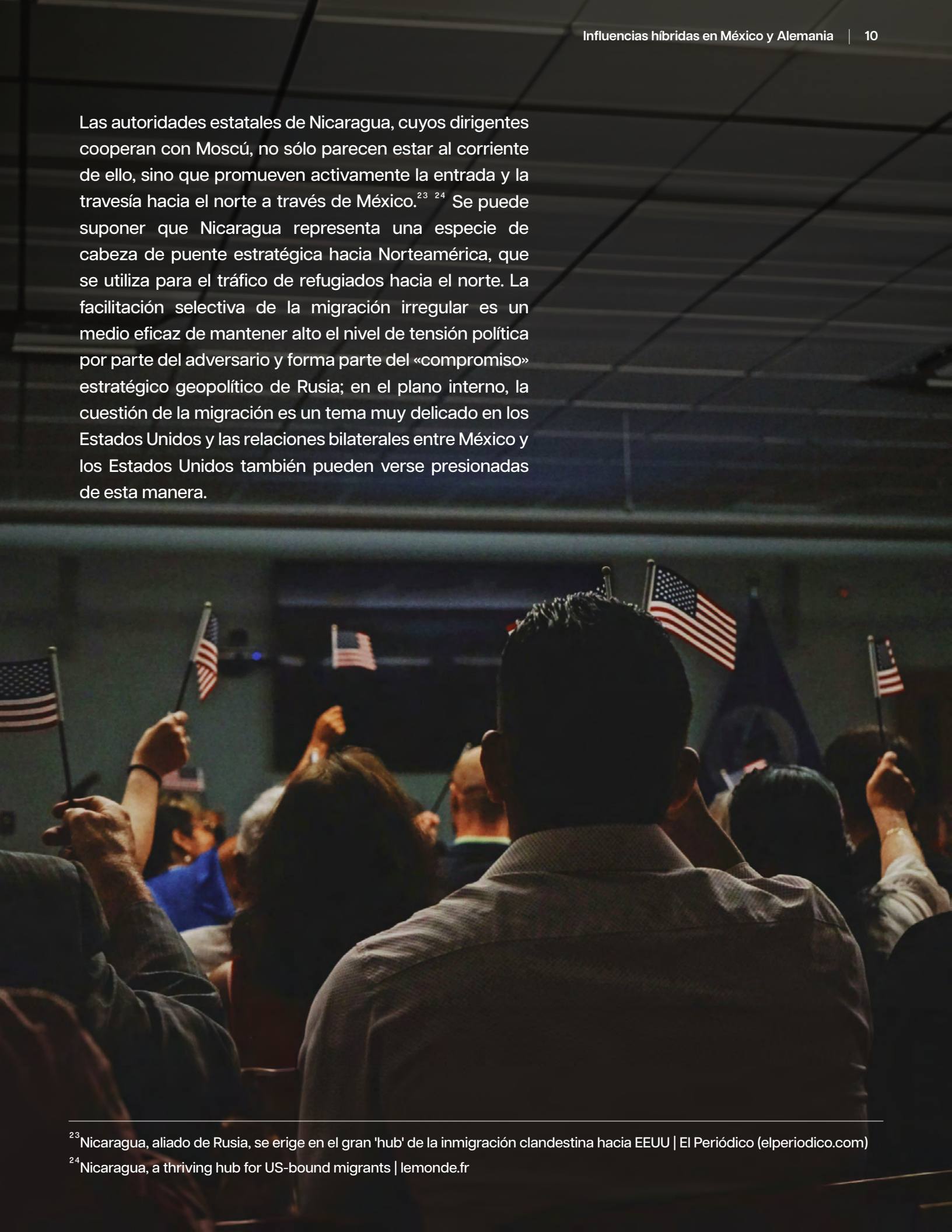
[19] Disinformation War Engulfs Mexican Presidential Race | Barron's (barrons.com)

[20] Mexico election: Sexist tropes and misinformation swirl online | AP News

[21] Experts warn against wave of fake news ahead of Mexico's 2024 presidential election | AP News

[22] Kremlin Disinformation Campaign Advances in Latin America - Diálogo Américas

Las autoridades estatales de Nicaragua, cuyos dirigentes cooperan con Moscú, no sólo parecen estar al corriente de ello, sino que promueven activamente la entrada y la travesía hacia el norte a través de México.[23] [24] Se puede suponer que Nicaragua representa una especie de cabeza de puente estratégica hacia Norteamérica, que se utiliza para el tráfico de refugiados hacia el norte. La facilitación selectiva de la migración irregular es un medio eficaz de mantener alto el nivel de tensión política por parte del adversario y forma parte del «compromiso» estratégico geopolítico de Rusia; en el plano interno, la cuestión de la migración es un tema muy delicado en los Estados Unidos y las relaciones bilaterales entre México y los Estados Unidos también pueden verse presionadas de esta manera.



[23] Nicaragua, aliado de Rusia, se erige en el gran 'hub' de la inmigración clandestina hacia EEUU | El Periódico (elperiodico.com)

[24] Nicaragua, a thriving hub for US-bound migrants | lemonde.fr

Estrategia nacional de prevención y respuesta

Para poder protegerse contra las amenazas híbridas, México y Alemania deberían estar preparados para las tácticas de sus oponentes y desarrollar un plan estratégico. La protección es una tarea de toda la sociedad y requiere la colaboración de todos.

1. Sensibilizar a la población

Es esencial que la sociedad esté informada y educada sobre las amenazas híbridas en términos de política de seguridad. Mientras que los sectores económicos están sensibilizados en primer lugar sobre los efectos inminentes de tales tácticas en sus procesos empresariales. No basta informar sobre la desinformación ni con la educación de los medios de comunicación. Hay que alcanzar a todos los sectores de la población. La información y la educación se pueden proporcionar a través de influenciadores para llegar a las generaciones más jóvenes, mientras que a las generaciones mayores hay que dirigirse a través de iglesias, festivales, supermercados y cafés de la ciudad. Además, el gobierno de Alemania y México podría proporcionar información sobre la situación de la seguridad en el país a través de declaraciones públicas semanales y así garantizar sucesivamente una mayor concienciación sobre las cuestiones de política de seguridad.

2. Reforzar las Medidas de seguridad

Además, las organizaciones gubernamentales y las infraestructuras críticas deben ampliar sus medidas de seguridad para aumentar el nivel de protección tanto digital como físico. Se puede minimizar el riesgo de responsables internos y reducir las oportunidades de sabotaje o espionaje realizando controles de seguridad a sus propios empleados. Las empresas tecnológicas y los desarrolladores de software deben integrar opciones técnicas (por ejemplo, aplicaciones de detección o marcas de agua) en sus dispositivos y servicios para facilitar la detección de información manipulada.

3. Adaptar las Estructuras

En términos institucionales, se necesita un centro eficaz y dinámico que tenga una visión de la situación. Un paso clave sería la creación de un centro de defensa híbrido. El centro debería incluir un centro de situación y análisis en el que se creara un panorama de la situación completo y actualizado diariamente. Mediante un tablero de control de la situación, se podrían registrar diversas áreas u objetivos de tácticas híbridas juntos y, si fuera necesario, situarlos en su contexto. La tendencia a combinar diferentes

tácticas permitiría una mejor visión de conjunto y una respuesta resumida a los impactos. Esto podría facilitar una vinculación más rápida entre un ataque a una operación de infraestructura crítica, como por ejemplo una central de abastecimiento de agua, y una campaña paralela de desinformación que intente difundir, por ejemplo, malas condiciones del agua o un riesgo de epidemia. Este tablero de situación incluiría el ciberespacio para los ciberataques, el espacio de la información para las campañas de desinformación e importantes servicios de suministro para las infraestructuras críticas (como la electricidad, el agua, la energía, Internet o el mercado financiero). En el marco de la consideración conjunta de las situaciones, los recursos también pueden ser desplegados de forma más rápida y flexible.

4. Tomar precauciones

Además, preparar a la población, los actores políticos y las empresas privadas ante situaciones de crisis es también una medida importante. La prevención para situaciones de estrés para el Estado, ya sean causadas por ciberataques o por ataques físicos contra infraestructuras críticas y la pérdida correspondiente de servicios de suministro vitales durante un cierto periodo de tiempo, es crucial para la resistencia y la resiliencia. Cuanto mayor sea la resiliencia, menor será el daño que puedan causar las tácticas híbridas. También da tiempo a las instituciones para reaccionar a los ataques. Los costos de las tácticas híbridas son bajos para los adversarios en relación con el daño potencial, ya que el nivel de resiliencia es aún muy bajo. El aumento de la resiliencia señala también a los oponentes que sus esfuerzos tendrán que ser mayores para lograr el efecto deseado. Esta tríada de prevención, detección y reacción es la base de la seguridad nacional en su conjunto.

Conclusión

Las amenazas híbridas suponen un reto fundamental tanto para México como para Alemania. Ambos países deben adaptar y fortalecer sus estrategias de seguridad para hacer frente con eficacia a estas complejas amenazas. Esto requiere una estrecha cooperación entre diversos actores estatales, sociales y privados, así como el uso de tecnologías avanzadas y sistemas inteligentes. En particular, la combinación selectiva de tácticas híbridas individuales puede sobrecargar rápidamente y perturbar significativamente la estructura del Estado. Sólo mediante un enfoque coordinado pueden Estados como México y Alemania preservar su soberanía y garantizar su seguridad frente a formas híbridas de influencia.

Autores

Mtro. Ferdinand Gehringer

Abogado en derecho y experto de ciberseguridad de la Fundación Konrad Adenauer. Exámenes jurídicos estatales de la Universidad Johannes Gutenberg, Mainz, y de la Tribunal Regional Superior, Frankfurt, Alemania. Egresado de la Universidad de Valencia, España.

Mtro. Maximilian Strobel

Maestro en Relaciones Internacionales y Diplomacia por la Universidad de Leiden en La Haya, Países Bajos. Licenciado en Ciencias Políticas y Filología Románica (español) por la Universidad de Mannheim, Alemania y la Universidad Autónoma de Madrid, España.

Referencias bibliográficas y electrónicas

- **Bundesministerium für Verteidigung.** (2024). Hybride Bedrohungen. https://www.bmvg.de/de/themen/sicherheitspolitik/hybride-bedrohungen
- **Hoffman, Frank G.** (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies. https://www.comw.org/qdr/fulltext/0712hoffman.pdf
- **Giannopoulos, G. & Smith, H. & Theocharidou, M.** (2021). The Landscape of Hybrid Threats: A Conceptual Model. Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf
- **NATO.** (2024). Countering hybrid threats. https://www.nato.int/cps/en/natohq/topics_156338.htm
- **Tagesschau.** (2023). Vermutlich russischer Hackerangriff auf SPD-Spitze. https://www.tagesschau.de/inland/innenpolitik/spd-hacker-russland-100.html
- **ZDF heute.** (2024). Merz-Daten bei Cyber-Angriff abgeflossen. https://www.zdf.de/nachrichten/politik/deutschland/cdu-cyber-angriff-merz-100.html
- **Spiegel Online.** (2024). Bundesregierung ordnet Hackerangriff auf SPD-Zentrale Russland zu. https://www.spiegel.de/politik/deutschland/bundesregierung-ordnet-hackerangriff-der-spd-zentrale-russland-zu-a-0f7d2fcc-630f-47d5-9a8f-c385a333a028
- **Auswärtiges Amt.** (2024). Deutschland im Fokus der pro-russischen Desinformationskampagne „Doppelgänger“. https://www.auswaertiges-amt.de/blob/2660362/73bcc0184167b438173e554ba2be2636/technischer-bericht-desinformationskampagne-doppelgaenger-data.pdf
- **Echtermann, A. & Jonas, U.** (2022). Gefälschte Regierungsdokumente und Nachrichtenseiten: Russische Desinformationskampagne nimmt Deutschland ins Visier. Correctiv. https://correctiv.org/faktencheck/hintergrund/2022/09/30/gefaelschte-regierungsdokumente-und-nachrichtenseiten-russische-desinformationskampagne-nimmt-deutschland-ins-visier-prigoschin/
- **Bayerisches Landesamt für Verfassungsschutz.** (2024). Interne Details zu russischer Desinformationskampagne „Doppelgänger“. https://www.verfassungsschutz.bayern.de/ueberuns/medien/-pressemitteilungen/desinformationskampagne-doppelgaenger/
- **Bundesministerium des Innern und für Heimat.** (2024). Schwerer Cyberangriff auf das Bundesamt für Kartographie und Geodäsie ist staatlichen chinesischen Angreifern zuzuordnen und diente der Spionage. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/07/cyberangriff-bkg.html
- **Sambale, M.** (2024). Berlin macht Peking für Cyberangriff verantwortlich. Tagesschau. https://www.tagesschau.de/inland/innenpolitik/ermittlungen-hackerangriff-bundesamt-kartographie-100.html
- **Yasmin, Abril M. Reis.** (2024). Evan Ellis: ‘Chinese engagement has taken on a more political and strategic tone in Latin America’. OPEU. Evan Ellis: 'Chinese engagement has taken on a more political and strategic tone in Latin America' - OPEU
- **Felbab-Brown, Vanda.** (2024). China, Mexico, and America’s fight against the fentanyl epidemic. Brooking. China, Mexico, and America's fight against the fentanyl epidemic | Brookings
- **Infobae. (2022).** Hydra Market: the financial nexus that linked Russia to the Mexican cartels. Hydra Market: the financial nexus that linked Russia to the Mexican cartels - Infobae
- **Juárez, Magali.** (2018). En elecciones del 2018, INE soportó el mayor ataque cibernético. El Financiero. En elecciones del 2018, INE soportó el mayor ataque cibernético – El Financiero
- **Beth Solomon, Daiana.** (2018). Cyber attack on Mexico campaign site triggers election nerves. Reuters. Cyber attack on Mexico campaign site triggers election nerves | Reuters
- **Abi-Habib, Maria.** (2022). Mexico Military Is Hacked, Exposing Abuse and Efforts to Evade Oversight. The New York Times. Major Mexican Government Hack Reveals Military Abuse and Spying - The New York Times (nytimes.com)

- **BBC News Mundo.** (2022). Guacamaya Leaks: 5 revelaciones del hackeo masivo que sufrió el ejército de México. Guacamaya Leaks: 5 revelaciones del hackeo masivo que sufrió el ejército de México - BBC News Mundo

- **Devanny, Joe & Buchan, Russel.** (2024). Mexico's National Cybersecurity Policy: Progress Has Stalled Under AMLO. Carnegie Russia Eurasia Center. Mexico's National Cybersecurity Policy: Progress Has Stalled Under AMLO - Carnegie Russia Eurasia Center (carnegieendowment.org)

- **Bravo, Miguel & Reta, Anella.** (2024). Disinformation War Engulfs Mexican Presidential Race. Barrons. Disinformation War Engulfs Mexican Presidential Race | Barron's (barrons.com)

- **Klepper, David.** (2024). Sexist tropes and misinformation swirl online as Mexico prepares to elect its first female leader. AP News. Mexico election: Sexist tropes and misinformation swirl online | AP News

- **Chacón, Marcos Martínez.** (2024). Experts warn against wave of fake news ahead of Mexico's 2024 presidential election. AP News. Experts warn against wave of fake news ahead of Mexico's 2024 presidential election | AP News

- **Pelcastre, Julieta.** (2024). Kremlin Disinformation Campaign Advances in Latin America. Diálogo Américas. Kremlin Disinformation Campaign Advances in Latin America - Diálogo Américas (dialogo-americas.com)

- **Marginedas, Marc.** (2024). Nicaragua, aliado de Rusia, se erige en el gran 'hub' de la inmigración clandestina hacia EEUU. El Periódico. Nicaragua, aliado de Rusia, se erige en el gran 'hub' de la inmigración clandestina hacia EEUU | El Periódico (elperiodico.com)

- **Montoya, Angeline et al.** (2024). Nicaragua, a thriving hub for US-bound migrants. Le Monde. Nicaragua, a thriving hub for US-bound migrants (lemonde.fr)

- **Portada: Fotografía del Auswärtige Amt en Berlin por Stephan Klonk.** Disponible en https://www.bundesregierung.de/breg-de/bundesregierung/bundesministerien/auswaertiges-amt

- **P.01: Fotografía de la Sede de la Secretaría de Relaciones Exteriores cortesía de SRE.** Disponible en https://www.jornada.com.mx/noticia/2021/06/15/politica/se-compromete-sre-a-atender-solicitud-de-pasaportes-del-ezln-8001

- **P.12: Fotografía del Auswärtige Amt en Berlin por Thomas Müller & Ivan Reimann Architekten.** Disponible en https://mueller-reimann.de/projekte/auswaertiges-amt-berlin