KONRAD
ADENAUER
STIFTUNG

The Institute
for Strategy &
Defense Research

Hybrid Influences in Mexico and Germany

Combining Hybrid Tactics as an Explosive Tool: How States Should Protect Themselves Against Modern Threats

Policy Brief

MA. Ferdinand Gehringer
MA. Maximilian Strobel

Abstract

Today's conflicts are no longer necessarily fought by military forces. Rather, 21st-century state actors, as well as non-state actors, seek to influence other states and their societies through flexible, dynamic, and diffuse strategies. Our world has changed radically, largely due to technological advances that make people's daily lives easier, but at the same time offer new points of access and venues for digital attacks.

The following report introduces hybrid tactics, what they are, and how they are used. Concrete examples of hybrid influence operations in Germany and Mexico are also included to illustrate the characteristics of these tactics and to show the political measures that both countries should urgently adopt and implement to better protect themselves in the future.

Destabilization through concealment and serious attribution

Hybrid tactics in modern conflict scenarios consist in the combined use of different instruments. The aim of these tactics is to influence state or interstate affairs, disrupt and destabilize societies, and/or influence public opinion.[1]

The actors involved can be both state and non-state. In this context, state actors in particular may also use private forces and criminal groups to achieve their goals and reinforce the cover-up of their actions. For this, these actors would require the means to exert covert influence, manipulation, or pressure (Hoffman, 2007). This makes attributing responsibility for an action much more difficult and is often only possible after some delay.

The actors operate below the threshold of armed confrontation. This means that their actions cannot be described as overt military attacks (Giannopoulos et al., 2021). Consequently, a (military) response in keeping with the law of war (ius ad bellum) is excluded. The "hybrid" label attempts to capture the phase between peace and war, often also referred to as the "state of discord". Therefore, the "hybrid" condition is not necessarily followed by the "war" condition (Hoffman, 2007).

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

Diverse exploitation of systemic weaknesses

The use of hybrid tactics is intended to weaken the opponent and influence their behavior. Ideally, these tactics compel the opponent to act in a way that serves one's own interests. This can be through political concessions, economic advantages, or the weakening of the opponent's international position (Giannopoulos et al., 2021).

Hybrid tactics target the opponent's systemic weaknesses. Actors exploit vulnerabilities in the social, economic, political, military, or technological spheres. There are about 40 different hybrid tactics. The main such tactics include cyberattacks and the exploitation of data breaches, attacks on critical infrastructure, economic pressure, targeted propaganda, disinformation, and migration.

Cyberattacks against IT infrastructure can steal data and information, paralyze systems, or spread disinformation. **Digital or physical attacks on critical infrastructure** can cripple operations and disrupt basic social and state services. Critical infrastructure includes energy and water supply, transport and traffic, information technology, and telecommunications.

Trade **sanctions, embargoes, or other economic measures** can be used to destabilize a country's economy or pressure the government to make certain concessions. Investments can also be considered a hybrid measure, as they are a means of gaining political influence and gaining control, like China's investments in infrastructure projects around the world.

The **selective dissemination of false or manipulated information** in the media and social networks aims to influence public opinion and aggravate social polarization.

Provoking, favoring or actively supporting **irregular migratory** movements can also be used occasionally to cause political, economic, or social instability in another state, as demonstrated by Russia's use of migration as a political weapon at the external borders of the European Union (EU).

Combination and accumulation as an explosive mixture

Individual tactics can cause enormous social, economic, and/or political damage. However, the biggest threat is undoubtedly the combination and accumulation of different tactics. An example of this is the combination of cyberattacks with disinformation campaigns to create political instability and undermine trust in democratic institutions.[2]

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

Such a scenario could play out as follows:

1. Cyberattacks on electoral infrastructure

Groups of hackers, possibly supported by foreign entities, carry out cyberattacks against the IT infrastructure that should guarantee the smooth running of elections. This can include hacking into voter registers and voting systems or paralyzing the websites of electoral commissions.

2. Spreading disinformation

Alongside cyberattacks, a disinformation campaign may be launched on social media and other digital platforms. This campaign could spread false information about voter fraud, manipulated election results, or alleged security breaches in election infrastructure.

3. Amplification through fake news and social media bots

To amplify the effect of disinformation, fake news articles are created and spread through social media bots and other fake or inauthentic accounts. These bots can automatically share, like, and comment on content to create the appearance of broad public support or social outrage.

4. Manipulative or manipulated videos and images

The use of *deepfake* technologies to create manipulated or fictitious videos and images that show political candidates in compromising or scandalous situations. This content is also distributed primarily through social media to undermine the public's trust in certain politicians.

5. Exploiting existing social and political tensions

Disinformation campaigns aim to aggravate existing social and political tensions in the destination country(s). In Mexico, for example, issues such as state corruption, violent crimes against innocents, and the behavior of drug cartels are deliberately addressed with partly falsified content to fuel fears, as well as mistrust or anger. In Germany, issues such as the treatment of migration and integration, the debate on skilled labor immigration, support for Ukraine in the Russian war of aggression, or support for Israel in the Middle East conflict have great potential for division.

Germany in the crosshairs of foreign actors

Germany and Mexico have very different political, geographical, and socioeconomic characteristics; However, both are attractive targets for hybrid influence by external actors, albeit with different approaches and intentions.

Germany is an attractive country for hybrid influence operations as it is a central player in the EU, Europe's largest economy, the logistics hub within the NATO alliance, and the most important site for U.S. forces outside the U.S. Aside from Russian influence through controlled disinformation campaigns, espionage, and attempts to sabotage critical infrastructure, China, Turkey, and Iran are especially active in Germany.

Last year, the email accounts of the ruling Social Democratic Party (SPD) and of sitting Federal Chancellor Olaf Scholz were attacked by hackers. In June 2023, the SPD announced that the accounts of the party's executive had already been the target of a cyberattack in January of that year. This was made possible by a security vulnerability in Microsoft software that was still unknown at the time of the attack. It is also possible that some data was leaked.[3]

A few months later, the Christian Democratic Union (CDU), currently the largest opposition party in Germany, suffered a cyberattack. Allegedly, data was also leaked in this case, including those of the party and parliamentary group leader, Friedrich Merz.[4]

Russian hacker group APT 28, with close ties to Russia’s military intelligence service GRU, was held responsible for the cyberattack on the SPD in Germany in April 2024.[5] The investigation into the attack on the CDU continues. Again, the authorities in charge of the investigation and prosecution assume a professional state agent was involved.

Since the beginning of Russia’s invasion of Ukraine in February 2022, a large-scale Russian disinformation campaign dubbed “Doppelgänger” has been active in Germany. The main goal of the campaign is to sow doubt regarding liberal democratic values and to question the foundations of the liberal democratic order by spreading deliberately false information and pro-Russian narratives.

[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

Specifically, the campaign is mainly aimed at discrediting German support for Ukraine. It includes deceptive-looking imitations of German news websites, such as Spiegel, Süddeutsche Zeitung, and BILD. Fake websites spread fake news, often on political issues, in order to fuel uncertainty and mistrust. Fake articles, some of which are created using generative artificial intelligence (AI), are then distributed through social media (e.g., through X, formerly Twitter, Facebook, YouTube, and TikTok) and other online platforms in order to maximize their reach. Another element of the campaign is the use of a complex technical infrastructure that includes servers rented from European companies. This infrastructure allows operators to host and distribute fake websites, content and hide their authorship.[6]

A concrete example of disinformation within the framework of the "Doppelgänger" campaign is the claims that weapons supplied to Ukraine end up on the black market in Germany.[7] Another example is fake news articles accusing the German government of freezing funds for pensions and social spending in order to finance the supply of weapons to Ukraine. Despite the efforts of European investigative authorities and platforms such as Facebook and Twitter/X to stop the disinformation campaign, it is still active.

The Bavarian Office for the Protection of the Constitution has carried out at least extensive technical analyses and has been able to get a meaningful idea of how the campaign works.[8]

At the end of 2021, the Federal Agency for Cartography and Geodesy (BKG) was the victim of a serious cyberattack attributed to Chinese state agents. The attack is a stunning example of espionage as a form of Chinese hybrid influence. Their goal was to steal sensitive data and infiltrate the BKG's network, highlighting the strategic importance of information gathering for China.[9] For example, the BKG provides geodata for some critical infrastructures (water, energy and transport companies) in Germany.[10]

The attackers used covert networks compromising the devices of private individuals and companies in order to cover their tracks and hide the origin of the attack. These types of cyberattacks undermine trust in state institutions and cyberse- curity, which can lead to long-term political and economic destabilization. The German government has strongly condemned the attack and summoned the Chinese ambassador, underscoring the diplomatic tensions that can arise from such cyberattacks.

[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

Mexico as a target and transit point for foreign influence

Mexico is a key player in Latin America; America's only southern neighbor was already a popular location for Russian spies during the Cold War and remains an attractive point of entry today: Russian secret service GRU is said to have more agents stationed there than in any other country.

The direct influence on Mexico itself, as a gateway or bridge to the United States, makes the country a transit point and a target for hybrid tactics. Russia and China, in particular, are trying to exert influence in Mexico and, through it, in the United States, also through regional allies such as Cuba, Venezuela and Nicaragua.[11] There are also suspicions that criminal groups from Russia and China are linked to powerful organized crime groups in Mexico.[12] [13]

There have already been reports of cyberattacks on the National Electoral Institute (INE) and political parties during the 2018 presidential campaign.[14] [15] Foreign agents were suspected of attempting to obtain sensitive information through hacking, disseminate it, and thus undermine the public's confidence in the electoral process and in the state institutions involved.

During the last television debate, the website of the opposition National Action Party (PAN) was paralyzed by an overload attack (the so-called DDoS attack). China and Russia were then suspected of being responsible for the cyberattacks.

In September 2022, six terabytes of stolen and highly sensitive information from Mexico's Ministry of National Defense (Sedena) were published.[16] An international hacker group called "Guacamaya" was responsible for the incident of the same name, Guacamaya Leaks, which was the largest data leak in the country's history. Secret communications between parts of the military came to light, as well as the known, but never proven, cooperation between politicians, security forces, drug cartels, and the judiciary. The Mexican military was exposed to public evidence of its increasing control over civilian government and infrastructure, gross institutional corruption, attempts to impede investigations into human rights violations, and the use of Pegasus spyware against journalists.[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

The hack continues to be an irreparable damage to the Mexican military, both internally and externally, and has resulted in underinvestment in cyber defense and political consequences.[18]

Disinformation campaigns are also a popular tool of selective manipulation in Mexico, especially during election campaigns; however, it is not very clear who is behind the spread of disinformation.[19] [20] In the run-up to the 2024 presidential election, the Mexican people were faced with an enormous amount of misinformation, particularly on social media. Among other things, candidate Claudia Sheinbaum was defamed for her Jewish roots; It was rumored that she would turn the country's most important basilica into a museum or that circumcisions would be mandatory under her presidency.

Last year, there was an increase in the selective dissemination of false information about the possible opposition candidate, Xóchitl Gálvez, according to which she would cut social programs for the poorest sectors of the population. President Andrés Manuel López Obrador (AMLO) regularly repeated this narrative in his morning press conferences. An interesting and different aspect of the campaigns in Germany is that the president himself is a central factor in the spread of false information in order to divide society. His allegations were spread online by sites with close ties to the government, a procedure that is also known in the United States.[21]

In addition, in recent years, Russia has significantly increased its media activities throughout Latin America, often with the aim of undermining the reputation of Western liberal democracies on the continent. Channels such as Sputnik Mundo and Russia Today (RT in Spanish) are notable examples of this clearly visible strategy; the Kremlin's geopolitical narratives and opinions (interpretations) are disseminated free of charge in Spanish through radio, television, the internet, and the written press with a professional coating. A common narrative is the portrayal of the West as interventionist, while authoritarian rulers such as Ortega in Nicaragua or Maduro in Venezuela present themselves as defenders of the sovereignty of their peoples – always implying that other countries risk being intervened if they do not remain vigilant. The openness of the media landscape in the region and the population's lack of knowledge about the media are exploited in this way. As a direct neighbor of the United States, Mexico is one of the main targets of Russian disinformation campaigns.[22]

Migratory movements can also be considered a hybrid threat under certain conditions, such as when they are deliberately facilitated. For example, it is clear that Nicaragua is an open hub for irregular migrants who are allowed to enter freely from Africa, India, Haiti, or Cuba to head north through Mexico.

[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

The Nicaraguan state authorities, whose leaders cooperate with Moscow, not only appear to be aware of this, but actively promote entry and passage north through Mexico.[23] [24] It can be assumed that Nicaragua represents a kind of strategic bridgehead to North America, which is used for the trafficking of refugees to the north. Targeted facilitation of irregular migration is an effective means of keeping the level of political tension high on the part of the adversary and is part of Russia's geopolitical strategic 'engagement'; domestically, the issue of migration is a very sensitive issue in the United States, and bilateral relations between Mexico and the United States may also be pressured in this way.

[23] Nicaragua, Russia's ally, becomes the great hub of clandestine immigration to the US | El Periódico (elperiodico.com)

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

National prevention and response strategy

In order to protect themselves against hybrid threats, Mexico and Germany should be prepared for the tactics of their opponents and develop a strategic plan. Protection is a task for the whole of society and requires the collaboration of all.

1. Raising awareness among the population

It is essential that society is informed and educated about hybrid threats in terms of security policy. The economic sectors are often the first to recognize the imminent effects of such tactics on their business processes. It is not enough to report on disinformation or rely solely on media education. There must be outreach to all segments of the population. Information and education could be provided by influencers to reach younger generations, while older generations need to be targeted through churches, festivals, supermarkets, and cafes in the city. In addition, the governments of Germany and Mexico could provide information on the security situation in the country through weekly public statements and thus successively ensure greater awareness of security policy issues.

2. Strengthen Security Measures

In addition, government organizations and critical infrastructure must expand their security measures to increase the level of both digital and physical protection. The risk of internal perpetrators can be minimized and opportunities for sabotage or espionage reduced by conducting security checks on employees. Technology companies and software developers should integrate technical options (e.g., detection apps or watermarks) into their devices and services to facilitate the detection of manipulated information.

3. Adapting Structures

In institutional terms, an effective and dynamic center with a vision of the situation is needed. A key step would be the creation of a hybrid defense center. The center should include a situation and analysis center, in which a complete and daily updated picture of the situation is created. Using a situation dashboard, various hybrid tactics areas or objectives could be recorded together and, if necessary, placed in context. The tendency to combine different tactics would allow for a better overview and a summary response to impacts. This could facilitate a faster link between an attack on a critical infrastructure operation, such as a water supply plant, and a parallel disinformation campaign that attempts to spread, for example, poor water conditions or an epidemic risk. This situation board would include cyberspace for cyberattacks, information space for disinformation campaigns and important supply services for critical infrastructures (such as electricity, water, energy, the internet or the financial market). Within the framework of the joint consideration of situations, resources can also be deployed more quickly and flexibly.

4. Take precautions

In addition, preparing the population, political actors and private companies for crisis situations is also an important measure. Prevention for state-stressed situations, whether caused by cyberattacks or physical attacks on critical infrastructure and the corresponding loss of vital supply services over a period of time, is crucial for resilience. The greater the resilience, the less damage hybrid tactics can cause. It also gives institutions time to react to attacks. The costs of hybrid tactics are low for adversaries relative to potential damage, as the level of resilience is still very low. Increased resilience also signals to opponents that their efforts will need to be greater to achieve the desired effect. This triad of prevention, detection, and reaction is the foundation of national security as a whole.

Conclusion

Hybrid threats pose a fundamental challenge for both Mexico and Germany. Both countries must adapt and strengthen their security strategies to effectively address these complex threats. This requires close cooperation between various state, social and private actors, as well as the use of advanced technologies and intelligent systems. In particular, the selective combination of individual hybrid tactics can quickly overburden and significantly disrupt the structure of the state. Only through a coordinated approach can states such as Mexico and Germany preserve their sovereignty and guarantee their security in the face of hybrid forms of influence.

Authors

MA. Ferdinand Gehringer

Lawyer, cybersecurity expert at Konrad Adenauer Foundation in Berlin. State legal examinations at Johannes Gutenberg University, Mainz, and Court of Appeal, Frankfurt, Germany. Graduated from the University of Valencia, Spain.

MA. Maximilian Strobel

Deputy Representative at Konrad Adenauer Foundation in Mexico. MSc in International Relations and Diplomacy from Leiden University, Netherlands. BA in Political Science and Romance Philology (Spanish) from Mannheim University, Germany and Autonomous University of Madrid, Spain.

Bibliographic and electronic references

- **Federal Ministry of Defence.** (2024). Hybrid threats. 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). Probably Russian hacker attack on SPD leadership. https://www.tagesschau.de/inland/innenpolitik/spd-hacker-russland-100.html

- **ZDF today.** (2024). Merz data leaked in cyber attack. https://www.zdf.de/nachrichten/politik/deutschland/cdu-cyber-angriff-merz-100.html

- **Spiegel Online.** (2024). German government attributes hacker attack on SPD headquarters to Russia. https://www.spiegel.de/politik/deutschland/bundesregierung-ordnet-hackerangriff-der-spd-zentrale-russland-zu-a-0f7d2fcc-630f-47d5-9a8f-c385a333a028

- **Foreign Office.** (2024). Germany in the focus of the pro-Russian disinformation campaign "Doppelgänger" https://www.auswaertiges-amt.de/blob/2660362/73bcc0184167b438173e554ba2be2636/technischer-bericht-desinformationskampagne-doppelgaenger-data.pdf

- **Echtermann, A. & Jonas, U.** (2022). Fake government documents and news sites: Russian disinformation campaign targets Germany. Correctiv. https://correctiv.org/faktencheck/hintergrund/2022/09/30/gefaelschte-regierungsdokumente-und-nachrichtenseiten-russische-desinformationskampagne-nimmt-deutschland-ins-visier-prigoschin/

- **Bavarian State Office for the Protection of the Constitution.** (2024). Internal details on Russian disinformation campaign "Doppelgänger". https://www.verfassungsschutz.bayern.de/ueberuns/medien/pressemitteilungen/desinformationskampagne-doppelgaenger/

- **Federal Ministry of the Interior and Community.** (2024). Serious cyber attack on the Federal Agency for Cartography and Geodesy can be attributed to Chinese state attackers and was used for espionage. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/07/cyberangriff-bkg.html

- **Sambale, M.** (2024). Berlin blames Beijing for cyber attack. 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). In the 2018 elections, INE endured the largest cyberattack. El Financiero. In the 2018 elections, INE endured the largest cyberattack – 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 World.** (2022). Guacamaya Leaks: 5 revelations of the massive hacking suffered by the Mexican army. Guacamaya Leaks: 5 revelations of the massive hacking suffered by Mexico's army - BBC News

- **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, Russia's ally, stands as the great hub of clandestine immigration to the US. El Periódico.. Nicaragua, Russia's ally, becomes the great hub of clandestine immigration to the US | 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)

- **Cover photo: Photography of the Auswärtige Amt in Berlin by Stephan Klonk.** Available for download here 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