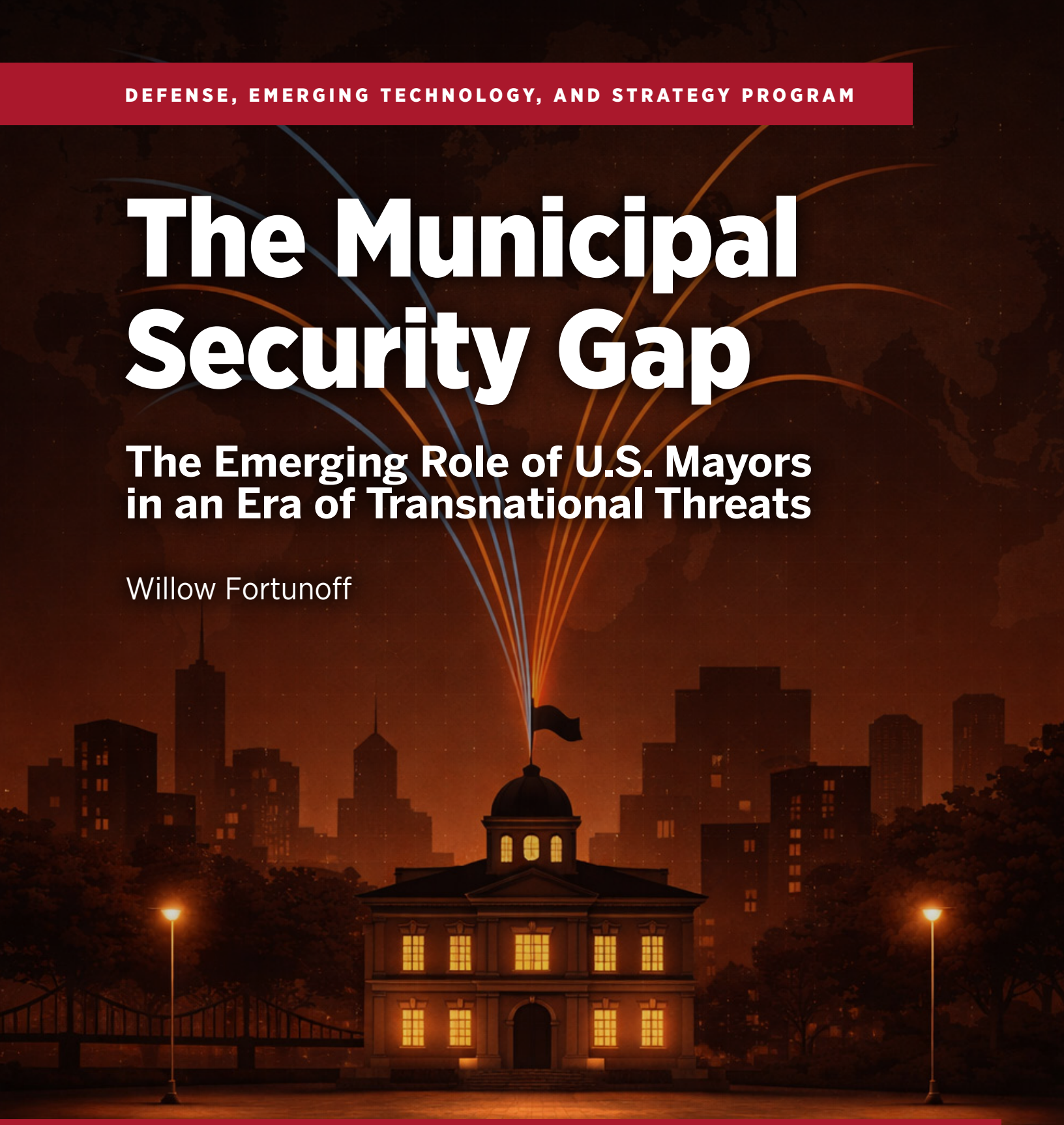
DEFENSE, EMERGING TECHNOLOGY, AND STRATEGY PROGRAM

The Municipal Security Gap

The Emerging Role of U.S. Mayors in an Era of Transnational Threats

Willow Fortunoff



HARVARD Kennedy School
BELFER CENTER

50 YEARS
OF RESEARCH, POLICY, AND LEADERSHIP

MARCH 2026

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org

DEFENSE, EMERGING TECHNOLOGY, AND STRATEGY PROGRAM

The Municipal Security Gap

The Emerging Role of U.S. Mayors in an Era of Transnational Threats

Willow Fortunoff

HARVARD Kennedy School
BELFER CENTER
50 YEARS OF RESEARCH, POLICY, AND LEADERSHIP

MARCH 2026

About the Defense, Emerging Technology, and Strategy Program

The Defense, Emerging Technology, and Strategy (DETS) Program advances knowledge at the nexus of security and technology while preparing students and fellows to be public service leaders. For more, visit belfercenter.org/programs/defense-emerging-technology-and-strategy.

About the Author

Willow Fortunoff is an MPP candidate at Harvard Kennedy School focusing on the evolving international engagement of U.S. mayors and governors. Recently, Willow worked for the UN Climate Change (UNFCCC) Global Climate Action team in Bonn, Germany, where she supported strategies to connect local governments to the international climate negotiation process. She was awarded a Fulbright research scholarship in Ecuador to study city diplomacy and migration and served as Assistant Director at the Atlantic Council's Adrienne Arsht Latin America Center in Washington, DC.

Willow has been published in *The Hague Journal of Diplomacy*, *The New Atlanticist*, and *The Routledge Handbook on Paradiplomacy*. She holds a B.A. in Political Science and International Studies from Macalester College and is the 2020 Truman Scholar from Vermont.

Table of Contents

Executive Summary 2

Introduction 4

Subnational Diplomacy and National Security 7

Transnational Criminal Organizations (TCOs) 11

- Threat Assessment 11
- Coordination Mechanisms and Governance Challenges 12

Cyber 18

- Threat Assessment 18
- Coordination Mechanisms and Governance Challenges 21

U.S.-China 23

- Threat Assessment 23
- Coordination Mechanisms and Governance Challenges 26

Cross-Cutting Case Studies 29

- New York City 29
- Houston 31
- Des Moines 32
- San Francisco 34

Recommendations 37

Conclusion 41

Endnotes 43

Appendix 1: Interview Table 50

Belfer Center/ Chat GPT

Executive Summary

Due to the size and global prominence of U.S. cities, many mayors are forging international relationships to advance local economic and cultural interests. As cities' global profiles rise alongside the spread of international security challenges, municipal governments have become more exposed to evolving risks. U.S. mayors are developing proactive responses to cybersecurity threats, transnational criminal organizations, and engagement with China. However, the traditional federal security system is not structured to address the decentralized nature of these challenges, allowing critical risks to fall through the cracks in local-federal security coordination.

Key Assessments

- **International security risks affecting cities are exposing gaps in U.S. policy and governance frameworks.** Cities increasingly bear the immediate impacts of emerging international threats, while national-security authority, intelligence, and strategic direction remain primarily federal. Mayors and local law enforcement are taking steps to build international partnerships and manage risks, but they often do so without standardized security frameworks or reliable federal support. This gap reveals two necessities: 1) making subnational security policies a core component of municipal international engagement, and 2) more systematically incorporating cities' exposure and governance role into national threat assessments and security strategies.

- **Threat information often reaches mayors too late and with limited utility.** Despite the Intelligence Community's duty to warn, threat information is shared inconsistently with municipal leaders and often after critical windows for early response have passed. Federal information-sharing mechanisms prioritize law enforcement and operational agencies, leaving elected officials with fragmented, event-driven intelligence that limits proactive coordination and risks damaging public trust when local leaders appear unprepared for emerging threats.

- **Federal-local law enforcement partnerships are essential but increasingly strained.** Cooperation is critical for addressing transnational crime and drug trafficking in cities, yet expanded federal involvement, particularly in immigration enforcement, has introduced governance tensions that can constrain local decision-making, erode community trust, and politicize joint

operations. Mayors remain publicly accountable for local impacts of federally driven actions, often without advance coordination or visibility into federal decision-making.

- **Municipal cyber defenses lag behind the scale of growing threats.** Cyberattacks against municipal governments are persistent and increasingly sophisticated, yet federal cybersecurity support has not kept pace with the scale of the risk. Federal funding reductions and policy uncertainty have weakened protections for election infrastructure and other critical local systems, leaving cities exposed and with diminished capacity to defend essential public services.
- **Structural asymmetries shape U.S.-China subnational engagement.** The People's Republic of China (PRC) has oversight and control over subnational diplomacy, while U.S. cities operate within a decentralized framework that prioritizes local autonomy and offers uneven federal guidance and administrative support. As U.S. cities engage internationally with fewer resources and risk-mitigation tools, they face growing exposure to geopolitical competition. Without clearer federal support and targeted capacity-building, these asymmetries are likely to continue shaping subnational engagement in ways that disadvantage U.S. local governments.

- **National leaders should support municipal security governance by institutionalizing nonpartisan pathways for information and resource sharing.** Federal agencies can formalize protocols for communicating significant national security threats to mayors, collaborate with trusted third-party organizations to develop guidelines for engagement with China, and adapt existing task force models to provide structured opportunities for city government input without compromising law enforcement independence.
- **City leaders should expand municipal security capacity by leveraging local expertise and peer networks.** Municipal governments can establish standing security commissions to improve horizontal and vertical coordination and develop risk-mitigation frameworks. These commissions should be supported by advisory councils that incorporate expertise from universities, the private sector, and diaspora groups. A dedicated national security task force within the U.S. Conference of Mayors could pool resources and ideas, such as the sharing of non-sensitive cybersecurity infrastructure templates and governance models among cities.

Introduction

In 2026, federal officials are no longer the sole U.S. government actors engaging in international relationships. The reach of global markets and technology began permeating borders alongside the flow of people in the 20th century, leading to urban hubs with worldwide economic and cultural influence. Mayors now play a proactive role in securing the benefits of international trade, cultural exchange, and tourism to their communities, while also broadcasting their city's unique attributes abroad. Los Angeles, as one example, has the third-largest metropolitan economy globally, with immigrant communities representing 34% of its population,[1] and processes over $268 billion in monthly international trade through its ports. Across the country, international engagement has become a necessary aspect of local governance – a trend underscored by more than 3,000 individual long-term partnerships and short-term initiatives between U.S cities, states, and foreign counterparts.[2]

International security and foreign policy strategies go hand in hand at the national level, yet the same is rarely true for city governments. In many cases, municipal leaders approach international engagement - including bilateral MOUs, engagement in networks, and sister city agreements - in isolation from public safety concerns, with asymmetrical or nonexistent frameworks for mitigating risks. Since subnational diplomacy has historically been viewed primarily as an instrument of "soft power," the role of cities in international security challenges has often been underestimated. A growing body of policy analysis highlights the issue of "city diplomacy risk" to describe how cities in democratic countries are exposed to geopolitical and competition challenges that they are not prepared to address.[3]

The issue of city diplomacy risk is clearly at play in the United States. The Intelligence Community's Annual Threat Assessment, a report presented to Congress by the Office of the Director of National Intelligence (ODNI), explicitly cited threats to municipal governments for the first time in 2025. While formal documentation has lagged, this signaled recognition of cities' vulnerability to international security threats previously considered to concern only national actors. In the words of Former National Cyber Director Harry Coker Jr, "I view them [state, local, tribal, and territorial governments] as being a combatant commander ... with many of us [federal agencies] being supporting commanders."[4]

The "supporting commanders" as referenced by Coker are primarily situated in the Department of State (DOS), the Department of Homeland Security (DHS), and the Department of Defense (DOD), and collectively advance the trifecta of diplomacy, public safety, and defense and deterrence. The "combatant commanders" in subnational governments are on the front lines of security challenges playing out in local communities. Yet Coker's analogy exposes a fundamental misconception between defense policy in a unified command system and a federal system. Combatant commanders exercise control over subordinate forces and capabilities. The president does not possess this authority over mayors and governors, who conduct domestic operations and international engagements with frequent but uneven federal support.

While subnational officials have increasingly deepened their engagement in diplomacy and public safety, defense and deterrence have not traditionally fallen within their remit. Emerging threats from foreign malign actors targeting local governments require stronger national coordination and support as these domains converge.

The landscape of current municipal security policy is currently dominated by three overarching challenges with localized impacts, which are magnified by globalization and engagement with international partners: 1) cyber-security, 2) drug trafficking and transnational criminal organizations (TCOs), and 3) managing relationships with China given inconsistent federal policy. These challenges were identified through synthesizing federal threat assessment reports and interviewing national security experts (see Appendix: Interview Table).

Counterterrorism has historically been the central focus shaping and codifying multi-level security coordination frameworks in the United States, especially after 9/11. Although foreign terrorist organizations still pose a threat, recent intelligence assessments emphasize that domestic actors now account for most terrorism risk, which distinguishes municipal responses from this paper's three main security challenges.[5] The traditional federal, state, and local security framework built in response to counterterrorism can be scaled to respond to more emergent and re-prioritized threats, as key vulnerabilities are falling through the cracks.

Of these issues, the federal response to TCOs and drug trafficking is the most institutionalized, yet it often lacks meaningful cooperation with mayors and international counterparts, which can destabilize public safety efforts. In contrast, domestic coordination on cybersecurity requires alignment with a wide array of private sector actors and is still developing. Engagement on U.S.-China relations at the subnational level is hampered by frequent policy shifts and a lack of clear protocols.

This report identifies a significant governance gap in municipal security oversight and offers recommendations for enhancing local-state-federal responses to security crises. Nearly every U.S. governor has an office of homeland security or emergency management, and the National Governors Association has a Homeland Security & Cybersecurity Program to provide technical assistance on "a range of national security policy issues."[6] This standardization does not exist at the municipal level.

The analysis finds that the local–federal security partnership model depends on a balance between federal resources and local knowledge. It can break down when federal initiatives are designed or executed with minimal local input or, conversely, when federal support is too limited to address transnational threats. The following sections examine how this balance is tested across cybersecurity, drug trafficking and transnational criminal organizations, and U.S.–China relations.

The report concludes with recommendations for bolstering security strategies across cities, a strategy which is both urgently needed and politically feasible. Mainstream political awareness of this issue has increased in recent years, with a 2024 Foreign Policy article emphasizing that "investing in subnational diplomacy isn't a luxury: It's imperative for national security."[7] As noted by the former Special Representative for City and State Diplomacy Nina Hachigian, "Making local officials more resilient to PRC approaches, fentanyl, cyberattacks—these are bipartisan issues."[8]

Subnational Diplomacy and National Security

Subnational diplomacy refers to the international engagement strategies pursued by local and regional government officials to advance economic, cultural, and political exchanges beyond traditional federal channels. These efforts include, but are not limited to, bilateral agreements with international governments to address shared priorities such as environmental programs and technology transfers,[9] sister city partnerships, participation in global networks, and trade missions. Recognizing the growing importance of these relationships, the U.S. government has made several attempts to institutionalize and coordinate a subnational diplomacy strategy—including the appointment of a Special Representative for Global Intergovernmental Affairs and Senior Advisor for Global Cities during the Obama administration and the establishment of the State Department's Unit for Subnational Diplomacy in 2022. Although the City and State Diplomacy Act has been introduced with bipartisan sponsorship in Congress multiple times since 2019, it has yet to be enacted into law. Without this legislative foundation, federal support remains informal and subject to executive priorities, rather than established in a permanent framework.

Fusion centers represent the most developed model for multi-level security coordination in the United States. These state and locally owned centers facilitate information sharing across levels of government and with private sector partners. Established in the years following the September 11 attacks, fusion centers were designed to strengthen nationwide threat detection and prevention by improving two-way communication between local law enforcement and federal agencies, including the Department of Homeland Security (DHS), Department of Justice (DOJ), and Federal Bureau of Investigation (FBI).[10] DHS designates statewide Primary Fusion Centers while statewide Homeland Security Officers can establish Recognized Fusion Centers in major urban areas – without any required approval from city officials. DHS assigns federal liaisons to share relevant intelligence at the appropriate clearance levels. Local law enforcement staffers are also trained as Fusion Liaison Officers to report Suspicious Activity Reporting (SAR) indicators to federal agencies.

Fusion centers initially focused on anti-terrorism efforts, but the nationwide model has faced criticisms and is poised at an inflection point. In 2012, the U.S. Senate Permanent Subcommittee on Investigations concluded a two-year bipartisan investigation into the approximately 70 established fusion centers. The Subcommittee's Ranking Member Sen. Tom Coburn (R-OK) argued that, "Instead of strengthening our counterterrorism efforts, they [fusion centers] have too often wasted money and stepped on Americans' civil liberties."[11] In practice, the SAR model has, at times, enabled reporting based on constitutionally protected activities and racial or religious descriptors rather than criminal behavior.

The establishment of 80 fusion centers has been at a standstill over the past five years and may decrease given federal funding cuts.[12] Leadership of the National Fusion Center Association recognize that the security environment has dramatically evolved since 9/11, and both the SAR indicators and process for engaging with local partners should also adapt.[13] Today, many statewide directors choose to focus on cybersecurity, drug trafficking, and adversarial interference at their own discretion, and the Association is working to develop updated indicators to guide a more even nationwide approach.[14]

While the "duty to warn" mandates that authorities in Intelligence Community (IC) entities notify officials who have a legitimate need for threat information to take protective action, this duty often results in inconsistent and delayed communication to municipal leadership. Fusion centers tend to focus on law enforcement and emergency management agencies rather than elected officials who must manage political, economic, and social implications of threats. When mayors do receive intelligence, it typically focuses on major events rather than detailed trend analyses, and because intelligence is heavily sanitized to protect sources, its informational value is often comparable to what mayors can obtain from public media.[15] **This fragmented communication can undermine mayors' ability to participate effectively in early threat response coordination and risks damaging their credibility with constituents.**

In 2025–2026, national attention has focused on ongoing legal challenges to President Trump's National Guard deployments to several U.S. cities. This paper does not propose changes to the national government's authority over national defense policy and armed forces, nor to state jurisdiction over their National Guard, but instead examines how mayors are responding to evolving threats within a constitutional system that gives the national government primacy over foreign and defense policy, and outlines changes that could enable cities to contribute more effectively to U.S. national security.

This paper takes the fusion center model's central premise - that effective vertical information sharing enhances national security - as its starting point. It explores how a more consistent, nationwide system of multilevel threat detection and preparedness could incorporate both political and security risks, while ensuring mayors are better informed and equipped to participate in security decisions that directly impact their communities.

The well-documented conflict between the Chinese firm Gotion, residents of a small Michigan township, and national political figures highlights significant shortcomings in the current approach—and the dramatic consequences of these failures. In 2022, Gotion moved forward with plans to establish a lithium battery component factory in Green Township, MI (population 3,200), with strong support from the township supervisor. However, when news of the project reached the community, it triggered widespread fears of Chinese Communist Party (CCP) interference. Rumors circulated about potential infiltration of the local college's cybersecurity program to gain access to government satellites, and there was anger over a foreign adversary receiving U.S. subsidies.[16] Subsequent reporting found no evidence to support claims of CCP infiltration or cybersecurity espionage, yet inadequate national security coordination and risk communication allowed these fears to escalate.

The case demonstrates gaps in local-federal security coordination. The federal interagency Committee on Foreign Investment in the United States (CFIUS), responsible for reviewing transactions involving foreign investment in U.S. businesses and certain real estate to determine their effect on U.S. national security, determined in 2023 that the proposed Gotion plant was not under their jurisdiction.[17] When Michigan Congressman John Moolenaar Former raised the Gotion plant during a Congressional hearing on cybersecurity, FBI Director Christopher Way noted that this type of project involving land and business acquisitions, while potentially legal, "can still raise national security concerns because it provides a vehicle for [China], if they want to leverage that access, to conduct surveillance or other operations that undermine our national security."[18]

While the next stage of this dispute remains uncertain, it has already resulted in the removal of all five former township board members from office and has cost the township at least $275,000 in legal fees in response to a federal lawsuit from Gotion.[19]

Three major conclusions can be drawn from this case that reinforce this report's importance:

1. Local assessments on foreign investment projects cannot solely consider economic merits but should also include national security assessments and transparent risk analysis.
2. A lack of institutionalized federal-local coordination can expose communities to unforeseen risks.
3. Public concern over national security, whether warranted or exaggerated, can jeopardize both local economic opportunities and the political prospects of local politicians.

Transnational Criminal Organizations (TCOs)

Threat Assessment

The 2025 Intelligence Community Annual Threat Assessment opens its analysis with the issue of Transnational Criminal Organizations (TCOs), while the 2025 Homeland Security Assessment warns that "the production, trafficking, and sale of illegal drugs by transnational and domestic criminal actors will continue to pose the most lethal threat to communities in the United States."[20] Mexican cartels wield the greatest influence in U.S. illicit drug markets, and drug trafficking and organized crime is a bilateral issue; both U.S. and Mexican communities contribute to the consistent supply and demand fueling this expanding market.[21]

The power and reach of Mexican TCOs in the United States have grown in tandem with the country's rising demand for illegal opioids – initially heroin in the 1980s and later fentanyl in the 2010s.[22] The Jalisco New Generation Cartel and Sinaloa Cartel operate transnational operations comprising of chemical sourcing from China, India, and Turkey, TCO alliances in Central American and Southern Cone port cities, and distribution into Europea and North America.[23] These Mexican-based TCOs are the largest producers and suppliers of illicit drugs to U.S. markets and typically smuggle through points along the U.S.-Mexico border using tactics such as mislabeled shipments. The U.S. Intelligence Community anticipates that border policy changes may catalyze new forms of delivery.[24]

Drug trafficking is not a one-way phenomenon; it is sustained by communities on both sides of the border. In recent years, drug traffickers have begun conducting final-stage fentanyl pill production in the United States.[25] In 2023, 86.4% of individuals sentenced for fentanyl trafficking were U.S. citizens.[26] This supply network has U.S.-based affiliates in major cities including Los Angeles, Phoenix, Houston, Chicago, Atlanta, and Miami responsible for recruiting their own traffickers.[27]

As Mexican TCOs respond to demands of drugs from the United States, U.S. gun manufacturers meet TCO demand for weapons. The U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) reports that almost three in four firearms

involved in crimes between 2022-2023 (73%) were trafficked illegally from the United States, and 82% of these "crime guns" were recovered in a state with dominant presence of the Jalisco New Generation or Sinaloa cartels.[28]

Coordination Mechanisms and Governance Challenges

The issue of TCOs and drug trafficking has a robust process of local to federal coordination, developed over decades of engagement. While mayors establish local law enforcement budgets and overarching priorities, a longstanding pattern of interagency cooperation operates largely independent of mayoral oversight. Police chiefs typically manage daily communication with state and federal agencies – including Drug Enforcement Administration (DEA), Federal Bureau of Investigations (FBI), Customs and Border Protection (CBP), and Department of Homeland Security (DHS) – often through task force frameworks focused on a specific issue.

However, these coordination mechanisms face evolving challenges. Staff turnover in local police and federal field offices frequently disrupts continuity in this "organic" communication, according to a senior CBP official.[29] The independence of law enforcement from political control is a fundamental safeguard of the American legal system. This separation also creates a governance challenge in which mayors bear political responsibility for outcomes shaped by decisions affecting their communities over which they have limited visibility or input.

Despite the high rate of U.S. citizen involvement in drug trafficking, federal responses are increasingly intertwined with immigration policy. The federal government typically collaborates with local officials through three approaches authorized under Section 287(g) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996: jail enforcement delegation, task force collaboration, and administrative warrant authorization. This policy allows ICE to delegate different roles to consenting local law enforcement officers, who typically can only stop or arrest individuals based on state laws.

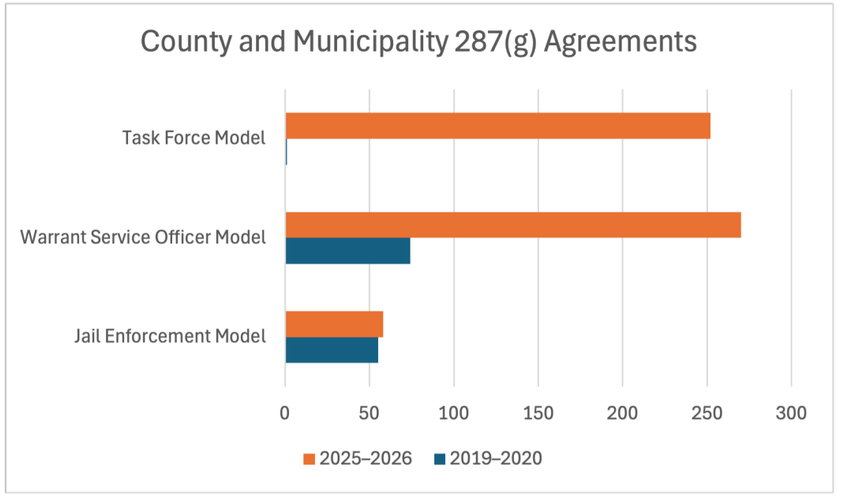
Task forces are the most common form of intergovernmental partnerships across all subnational levels. The High Intensity Drug Trafficking Areas (HIDTA) program, created in 1988 and administered by the White House Office of

National Drug Control Policy, provides funding to selected law enforcement agencies and places operational direction under joint Federal and non-Federal law enforcement.[30] Homeland Security Initiative's Border Enforcement Security Task Force (BEST) was created in 2005 to connect local and federal investigations combatting TCOs. While local police departments can assign officers to BESTs, the investigations and decisions are determined by HSI. The "Vulcan" task force launched in 2019 to target one specific TCO, Mara Salvatrucha (MS-13), operates under Department of Justice leadership with support from the FBI, HSI, and DEA, with limited local operational input.[31]

The federal focus on TCOs has intensified under the second Trump administration. In January 2025, President Trump designated eight TCOs - including MS-13, the Jalisco New Generation cartel, and Sinaloa cartel - as Foreign Terrorist Organizations (FTOs) and Specially Designated Global Terrorists (SDGTs). These actions give federal authorities expanded tools, particularly asset freezes and immigration consequences, to pursue cartel leadership and facilitators, potentially shifting the balance of authority toward federal prosecutors in cases that might previously have been handled primarily as drug or organized crime matters at the state and local level. In 2025, the Department of Justice launched "Operation Take Back America," a nationwide initiative that leverages the Organized Crime Drug Enforcement Task Forces (OCDETF) and other frameworks to coordinate investigations and prosecutions against cartels and other transnational criminal organizations. Early prosecutions under the initiative have focused on narcotics, firearms, and immigration offenses and officials have publicly signaled an intent to use terrorism-related authorities more aggressively in cartel cases as the new designations are operationalized.[32]

During the second Trump administration, the number of section 287(g) agreements signed with counties and municipalities has increased by nearly 3.5% according to ICE data (See Figure 1 below). The task force model, curtailed in 2012 by President Obama due to concerns of racial profiling and civil rights violations, was reinstated in early 2025, along with expansions of all Section 287(g) approaches.[33] The task force model has the broadest delegated authorities and remains the most controversial. The warrant service officer approach is still more common with city and county partnerships local officers to serve and execute ICE administrative warrants on people already identified and already in custody, and the jail enforcement approach has historically been the most consistently used model.

Figure 1



Caption: Available data from Immigration and Customs Enforcement (ICE) (https://www.ice.gov/287g) tracks new Section 287(g) agreements signed in 2019, 2020, 2025, and 2026.

Growing evidence shows that Section 287(g) agreements create community tensions that can undermine drug interdiction objectives. A 2019 study revealed that deputizing immigration duties to local police significantly reduces undocumented immigrants' trust in local enforcement officials.[34] This "chilling effect," where community members become reluctant to engage with authorities, can decrease security cooperation with communities who may be knowledgeable about TCO presence. The Police Executive Research Forum confirms that increased fear and distrust contribute to immigrant communities' reluctance to report crimes or cooperate in investigations.[35]

A prime example of how rapidly an imbalanced federal-local partnership can imperil public safety exists in the large-scale federal immigration enforcement campaign in Minneapolis beginning in late 2025. In January 2026, federal immigration agents shot and killed two U.S. citizens, Renée Good and Alex Pretti, prompting thousands of people to protest in Minneapolis and across the country.[36]

Governor Tim Walz and Minneapolis Mayor Jacob Frey have characterized the surge of more than 2,000 federal agents as crossing a "significant and terrifying line" and called for de-escalation.[37] While Minneapolis has traditionally cooperated with numerous federal agencies to combat crime, Chief Justice Patrick Schilt ruled that recent federal actions have violated at least 96 court orders.

The U.S. Conference of Mayors released a bipartisan statement arguing that "deadly confrontations like these erode public trust in law enforcement at every level, putting our own local police officers across the nation at added risk,"[38] with Mayor Frey adding that "a lot of repair that needs to be done with the trust that has been damaged by this federal government."[39]

The February 2026 lapse in DHS funding highlighted deep partisan disagreement over the terms of federal-local security cooperation, with Democrats calling for new oversight and restrictions governing federal immigration enforcement and many Republicans arguing that restrictions should be placed on cities and states that limit cooperation with immigration authorities.[40]

More broadly, the escalation of federal involvement in local governance presents mayors with a grave dilemma. On one hand, increased federal coordination can bring additional financial and technical resources to address TCO and drug trafficking threats. Evidence from drug-market research suggests that when local policing only focuses on apprehending low-level dealers, it has limited impact on overall drug market supply.[41]

On the other hand, aggressive federal operations can constrain local governments' ability to set priorities and maintain legitimacy within their own jurisdictions. Compliance with federal immigration directives can lead to officer shortages and community tensions, while political accountability for federally driven operations often falls on mayors and police chiefs who have limited operational control and visibility. The structure of agreements with federal agencies can therefore undercut objectives of detecting drug traffickers and fentanyl trade if approaches ignore community relationships and local intelligence. According to Republican mayor Jerry Dyer, federal immigration agencies are using policing tactics "that have been abandoned by local law enforcement 30 years ago."[42]

This issue can place mayors in an exceptionally complex position and led many cities to pass "sanctuary" policies over the past decade. Mayors and police chiefs frequently argue that assuming immigration enforcement responsibilities can compromise their primary public safety mission by discouraging criminal intelligence from witnesses and victims of crime.[43] Sanctuary policies typically

limit cooperation and information sharing with federal agencies. In response, the Trump administration has repeatedly sought to penalize these jurisdictions. In 2025, the Trump administration accused dozens of cities and counties across 37 states and the District of Columbia for being non-compliant with Federal rules, including noncompliance with Federal law enforcement in enforcing immigration laws and restrictions on information sharing.[44] Federal officials argue that these local limits on cooperation can be detrimental for officer safety.[45] In short, local and federal law enforcement are mutually dependent in responding to these complex threats.

Political alignment between local and federal executives further complicates these dynamics. Mayors face pressure from below, as constituent preferences to seek or reject federal partnerships based on partisan considerations can run counter to practical law enforcement needs. They also are scrutinized from above, as national political officials often target local officials of a different political affiliation. For example, the Mayor of Nashville, TN faces a federal investigation led by House Republicans due to an executive order requiring city officials to disclose interactions with ICE to the mayor's office amidst increased ICE raids.[46] The Trump administration opened investigations into both the mayor of Minneapolis and governor of Minnesota for an alleged conspiracy to impede federal agents.[47] These dynamics can weaken the coordination and intelligence-sharing on which both federal and local authorities depend.

Recent federal actions have impacted the availability of TCO investigation support and may cause significant local challenges in the coming months. A November 2025 New York Times investigation found that "thousands of agents" who typically investigate TCOs have been reassigned to immigration enforcement duties.[48] This reduction in federal support for TCO detection, in conjunction with reduced voluntary reporting from affected communities, is likely to leave mayors and local law enforcement agencies with critical information and resource gaps.

There have been several approaches at deepening international subnational cooperation along the border, yet these initiatives lack consistency and integration into national policies. The U.S. - Mexico Border Mayors Association was established in 2011 to enact "shared programs and enhanced information sharing...to focus law enforcement attention on those who most merit it"

including "exchanging passenger information to detect and detain possible drug and weapons smugglers." The Association also aimed to "initiate pilot pre-clearance, pre-screening, and pre-inspection program for drug detection" and increase overall binational law enforcement cooperation.[49] After six summits, mayors noted "Unfortunately, there is an absence and lack of unity of organizations like ours to speak for the border. Our voices have not been heard. We have been left out of the discussion." They issued a call for local government leaders to "unite and integrate horizontally across the border."[50] While ad-hoc gatherings have formed in recent years, such as the Sister Cities International's U.S.-Mexico Mayors' Community Forum and the North American Mayors Forum, the U.S.-Mexico Border Mayors Association has not met publicly since 2019.

It is clear that mayors lack a consistent mechanism for international and national coordination regarding drug trafficking and TCOs. Local officials in the U.S. also engage in consistent cross-border diplomacy with Mexican counterparts based on necessity, but this partnership could include a greater focus on security concerns. Mexico has 50 consulates in major cities across the United States, and they conduct public diplomacy through partnerships with local governments, universities, and companies.[51] On both sides of the border, mayors are the government officials with the closest access to gun manufacturers. While municipal gun control policies are preempted by state and federal policy, mayors can leverage their limited authority to drive normative and policy changes. U.S. cities that are home to gun manufacturers can mandate security requirements, such as video surveillance of stores and mandatory reporting of lost or stolen firearms.

Cyber

Threat Assessment

Local governments and their public utilities are both high impact and highly vulnerable targets for cyberattacks, described by Former United States Director of the Cybersecurity and Infrastructure Security Agency Jen Easterly as "target rich but cyber poor."[52] In 2025, the primary threats facing municipalities included ransomware attacks, the targeting of election infrastructure, and rapidly evolving risks associated with artificial intelligence (AI). The former executive assistant director for the FBI Information and Technology Branch cyber claims that "a focused disruption can be potentially life-threatening when considering the health and public safety services our local governments control."[53] In the face of this escalating threat landscape, S&P Global Ratings has reportedly considered downgrading municipal ratings for cities with weak cybersecurity.[54]

Given the essential and often time-sensitive nature of municipal service delivery, city governments make a prime target for ransomware attacks. In fact, ransomware remains the most prevalent and disruptive cyber threat to local governments.[55] In 2024, over 30% of state and local governments reported experiencing at least one cyberattack, with ransomware incidents causing prolonged outages of 911 dispatch, public utilities, and other essential services.[56] The 2025 IC Annual Threat Assessment spotlights municipal governments as being "inadequately defended" against these escalating threats, which leads to escalating costs.[57] While only 5% of local governments paid recovery payments exceeding $1 million in 2022, the average cost of a single attack in 2024 had risen to $2.83 million.[58]

Many cities still rely on outdated systems that lack modern security features and make them easy targets for hackers.[59] As municipal governments migrate data and processes online, they must continuously update and secure their systems to avoid vulnerabilities inherent in legacy IT infrastructure. However, many cities lack the funding to implement sufficient technical refreshments, which can lead to systemic weaknesses. In May 2025, a Chinese-speaking group exploited a gap in older versions of Cityworks, a platform used widely by state and local governments to manage water and waste systems.[60] It was estimated that approximately one in five publicly accessible Cityworks deployments were vulnerable to this flaw.[61] This

was not a ransomware attack; instead, the group engaged in cyber espionage by mapping utilities management systems and accessing confidential information, while also establishing backdoors for long-term access.[62]

The rapid adoption of "smart city" solutions - such as integrating IoT sensors ("Internet of Things" hardware devices that transfer data on physical world to digital platforms), cloud-based platforms, and AI-powered analytics - has enabled cities to streamline government operations, improve accessibility of service delivery, and reduce costs. However, this digital transformation dramatically expands the attack surface for cybercriminals, as each new connected device–whether a water meter or surveillance camera—represents a potential entry point for malicious activity. Alarmingly, 98% of IoT device traffic is unencrypted.[63] This means that sensitive data can be easily intercepted or manipulated as it travels across city networks. Digitalizing government services without an accompanying focus on encryption and cybersecurity can risk exposing critical infrastructure and civilians' private information to exploitation.

Advancements in AI present exponentially increasing opportunities and risks for city governments. AI-powered tools, such as predictive threat detection and automated incident response systems, can allow municipalities to identify vulnerabilities faster than human teams alone. For example, AI-driven network monitoring can flag anomalous traffic patterns indicative of ransomware or espionage campaigns to allow cities to mitigate breaches before systems are compromised.

These same AI technologies can also be weaponized by adversaries to erode local government processes. AI-generated deepfakes, for instance, can spread disinformation about candidates, as seen in the case of a Chicago mayoral candidate in 2023.[64] AI can also enable attackers to automate cyber penetration testing in order to find and exploit system weaknesses much faster than human capabilities.[65]

Municipal and county elections remain a prime target for foreign actors aiming to subvert and influence U.S. democratic processes. In 2016, the Russian government led a major cyberattack campaign on "dozens" of state and local governments.[66] In 2020, Iranian hackers probed state and local websites as part of an effort to gain access to voter data, and were successful at gaining access to a voter registration database in one state.[67] While these localized attacks may not swing an entire national election, they can have significant impacts on local politics and also spread mistrust in the electoral process.

These attacks are often spearheaded by geopolitical adversaries as part of a national security strategy. While China is regarded as the most active cyber threat, other adversaries also use cyber tools to advance their interests. Iran, for example, has used cyber filtration in municipal water and waste systems. Experts note that, at this point, their efforts seemed aimed at demonstrating their access.[68] Iran has also targeted local governments with the goal of deploying ransomware and stealing sensitive data, including against organizations focused on or based in Israel.[69] Russia has used cyber disruptions as a foreign policy lever, and has activated SVR cyber units, such as Nobelium (also known as Cozy Bear) to conduct cyberattacks against the U.S. and Europe as a core aspect of its Ukraine invasion efforts. While these efforts predominately targeted logistics and IT companies involved in aid delivery,[70] they illustrate the broader risk to critical infrastructure in municipalities. Many countries, including North Korea, are maturing their cyber capabilities and may adapt their targeting strategies based on the perceived success of attacks by other nations. As a result, local governments should anticipate an evolving landscape of persistent and increasingly sophisticated cyber threats.

A former senior official at the National Security Council's Cybersecurity Office claimed that "localized attacks are not one-off instances" but are instead part of a broader effort to "systematically determine our [the United States] vulnerability."[71] **Many of the individual ransomware attacks and backdoor attempts targeting municipal governments and civilian infrastructure across the country should be understood as a more comprehensive effort to test approaches and identify weak links in U.S. cybersecurity.** At the aggregate level, the scale and frequency of these incidents indicate that the country is already amidst a crisis.[72] Former FBI Director Christopher Wray reinforced this point by observing that cybersecurity attacks from China in particular are "not focused just on political and military targets" but that "low blows against civilians are part of China's plan."[73]

Coordination Mechanisms and Governance Challenges

The threat of cyberattacks against municipal governments has gained attention over the past five years, yet federal support has not been proportional to the issue. During the high-profile attacks against election infrastructure in 2016, state and local officials claimed that they had not received warnings from the federal government that they had been targeted.[74] In 2019, a nationwide survey found that municipalities were "under frequent, if not constant, attack" and showed poor cybersecurity practices in the aggregate.[75] That same year, the Senate Permanent Subcommittee on Investigations found that "[Federal]" Agencies currently fail to comply with basic cybersecurity standards."[76]

Federal support for local cyber defense made great strides under the first Trump and Biden administrations. In 2018, Congress established the Cybersecurity and Infrastructure Security Agency (CISA), and CISA's first Director noted in 2021 that "state and local governments simply cannot protect themselves... We have to make that generational leap in technology, and the federal government has to help here."[77] In 2021, the Bipartisan Infrastructure Law established the State and Local Cybersecurity Grant Program (SLCGP), which aimed to provide $1 billion over four years, with an 80% pass-through requirement to local governments. The Secretary-Treasurer for the National Association of Chief Information Officers noted that, in addition to supporting concrete IT projects, this program catalyzed a narrative shift, where municipalities felt emboldened to report incidents to the state with less fear of punitive action.[78] In 2024, the OMB updated its Uniform Guidance policy to permit federal funds to be used for data costs including cybersecurity.[79]

The second Trump administration restructured funding opportunities in response to political priorities. In March 2025, CISA cut more than $10 million in funding to two cybersecurity intelligence-sharing programs that supported state and local governments: The Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), both managed by the Center for Internet Security, a non-profit supporting 18,000 state and local government members. [80] EI-ISAC was launched after high-profile threats of Russian election interference. Notably, both MS-ISAC and EI-ISAC were intentionally structured outside direct federal control to address civil-liberties concerns while sharing largely unclassified but operationally valuable cyber threat information. In the final year of the SLCGP, DHS barred grantees from using funds for any costs associated with the Center for Internet Security, effectively defunding both initiatives.[81] The SLCGP is set to expire at the end of January 2026, and the Trump administration has cut staff at the federal agencies managing the program.

The reduction in federal support has further strained municipal capacity to defend against increasingly sophisticated threats. According to a Republican secretary of state, "Withdrawing CISA's support for local election officials will make elections less secure."[82] Over half of the Center for Internet Security's funding was cut by the Department of Government Efficiency (DOGE).[83] When asked about potential future CISA cuts in 2024, Former United States Director of the Cybersecurity and Infrastructure Security Agency Jen Easterly said, "It would have a catastrophic impact on our ability to protect and defend the critical infrastructure that Americans rely on every hour of every day."[84]

The U.S. Conference of Mayors has attempted to partially fill this policy gap, yet their own efforts are currently constrained by a lack of federal resources. In 2019, the Conference adopted a resolution opposing payments after ransomware attacks based on the argument that payments incentivize further attacks.[85] The current President of the Conference, Mayor Ginther of Columbus, Ohio, has made cybersecurity a top priority, with a focus on returning federal funding. The Conference joined other local government associations in sending a letter to congressional leaders in September 2025 asking to reauthorize the SLCGP.[86]

U.S.-China

Threat Assessment

The People's Republic of China (PRC) has actively encouraged subnational relationships with the United States since the early 21st century, and these relationships have become increasingly weaponized and scrutinized in the past eight years amidst heightened U.S.-China geopolitical tensions.[87] Federal reports find that the PRC seeks to increase subnational engagement and posits that the "scope and scale of PRC influence, recruitment, and elicitation efforts may increase as these engagements grow."[88] The U.S. Intelligence Community has estimated that Beijing's strategy stems from a belief that "local officials are more pliable than their federal counterparts."[89] Today, the PRC subnational strategy is largely directed at controlling pro- Chinese Communist Party (CCP) cultural narratives, collecting intelligence, advancing pro-CCP local policies by supporting political candidates, and seeking crucial footholds in the U.S. economy as points of leverage.

The international security threat posed by China is broad, and the challenge faced by mayors involves multiple dimensions that require varied strategies. PRC operations encompass intelligence threats, Chinese ownership of property, involvement by Chinese companies in ports, cyber threats, economic espionage, monitoring of Taiwan-related interests, and cultural initiatives aimed at expanding soft power.

The different political structures of the U.S. and the PRC help explain the potential for asymmetric subnational relationships. The PRC treats subnational diplomacy as an extension of national foreign policy and closely monitors international engagement of local officials through party-state institutions such as the United Front and Chinese People's Association for Friendship with Foreign Countries (CPAFFC).[90] By contrast, the United States' decentralized and historically open approach to city and state diplomacy has enabled deep, decades-old relationships supported by numerous local stakeholders, including universities and volunteer associations. In the U.S., international engagement outside of formal treaties is determined by local officials, who have the autonomy to visit and host Chinese counterparts without a standardized national protocol.

At present, these systematic differences have resulted in lopsided administrative and staffing capacity for subnational diplomacy. All major Chinese cities have a Foreign Affairs Office, and the ratio of Chinese to U.S. international relations staff in municipal offices can reach 100 to 1.[91] As Mareike Ohlberg, senior fellow at the German Marshall Fund, has observed, "There's been quite a mismatch in terms of resources on the PRC side vs U.S. side."[92]

President Xi Jinping has prioritized the advancement of the United Front Work Department (UFWD) which he describes as a "magic weapon" for the success and rejuvenation of the CCP.[93] UFWD is a CCP central government organ which monitors adherence to CCP values and interests across provincial and local party committees, as well as academic institutions and companies in China. The UWFD also manages the "united front" – an "amorphous network" of CCP officials and U.S.-based grassroots organizations with a collection of tactics aiming to promote China's influence and extend their domestic mandate abroad.[94] Historically, much of this work has promoted cultural exchanges between students and local government leaders. For example, the United States Heartland China Association organized a delegation of six mayors to China in 2023,[95] while the China Education Association for International Exchange sponsors high school exchanges.

The united front can also mobilize diaspora groups in U.S. cities for more subversive aims, including co-opting and neutralizing any threats of an autonomous Chinese civil society and blocking anti-CCP initiatives in the United States. These groups typically host cultural events and business networking functions which can also be a "smokescreen for political espionage."[96] For example, when President Xi Jinping came to California, United Front mobilized Chinese Americans to block Tibetan demonstrators who planned to protest.[97]

The united front's mobilization efforts have increasingly focused on achieving political wins. Associated civic organizations work to cultivate preferred candidates in Asian American districts, starting at local levels of government.[98] Their campaigning has supported the election of at least three Democratic and Republican local politicians in South Brooklyn over the past three years, and groups have also used opposition efforts to target Taiwanese American politicians.[99] Growing awareness of the united front's political leverage has also spawned xenophobic and anti-Asian discrimination, where accusations of being CCP plants have become a campaign tactic.[100]

The targeting of Taiwanese American candidates is part of a broader anti-Taiwan battle playing out across one of the most quintessential "soft power" policies: sister city agreements. These agreements, popularized beginning in the 1950s, typically focus on cultural exchanges and public events, with some evolving to focus on economic and diaspora ties.[101] CPAFFC is responsible for overseeing all sister relationships and often require agreements to refer to the One China Principle.[102] U.S. cities are under no such directives. According to a former State Department official, this information asymmetry has come back to haunt U.S. city officials who receive angry letters or phone calls from Chinese consulates and officials following perceived engagement with Taiwan.[103] In 2020, two U.S. Senators claimed that "Sister-city partnerships may leave American communities vulnerable to Chinese espionage and economic coercion."[104]

The CCP's cultural and political priorities are intertwined with efforts to boost China's economic competitiveness through enhanced trading relationships and access to critical economic intelligence. DHS refers to their approach as a form of "economic espionage" where CCP officials work to form subnational economic agreements, sometimes framed within sister-city agreements or Memoranda of Understanding (MOUs), to facilitate increased trade partnerships. Foreign Direct Investment, a key priority for U.S. mayors, can be exploited to gain access to critical infrastructure and sensitive technology[105] or threatened to be withdrawn if the U.S. city acts unfavorably.[106]

A common challenge for U.S. officials engaging with Chinese counterparts is a lack of clarity regarding long-term motives and short-term expectations of agreements, as well as the potential for malign intentions of Chinese actions. Chinese officials typically require MOU agreements to state "in accordance with the principles on the establishment of diplomatic relations between the United States of America and the People's Republic of China."[107] While potentially innocuous, this line is in reference to the One China principle and can be used to justify any pushback against future U.S. subnational engagement with Taiwan. The Subnational Diplomacy Unit at the Department of State observed that CCP frequently has a transactional approach to subnational relationships and will enter into panda exchanges or sister city agreements as a tool of leverage, and the desired outcome isn't always clear for local U.S. officials.[108]

Coordination Mechanisms and Governance Challenges

Senior intelligence officials across multiple administrations have acknowledged that the PRC seeks to exploit subnational relationships to advance its geopolitical interests, though federal policy responses have diverged in how to manage this risk. The first Trump administration (2017 – 2021), urged greater caution in subnational engagement and focused on increasing federal oversight of PRC diplomatic outreach. Former Secretary of State Mike Pompeo told governors that "competition with China is not just a federal issue," arguing that "the cumulative effect [of Chinese competition at the local level] is of enormous national importance and international significance."[109] During this period, Pompeo made a series of speeches around the country warning of subnational engagement with China, and the State Department imposed policies requiring Chinese diplomats to provide advance notification and prior approval, in some cases, ahead of official meetings with state and local officials.

The Biden administration (2021-2025) maintained concern about PRC influence while shifting toward a facilitative, risk-management approach. A 2022 report from the National Counterintelligence and Security Center articulated a nuanced view that PRC influence operations can be "deceptive and coercive" while also acknowledging that, for many U.S. state and local communities, "engaging with counterparts in China may be necessary or even vital."[110] Rather than discouraging subnational engagement outright, the State Department's Unit for Subnational Diplomacy supported city officials by offering briefings from China House experts and facilitating pre-meeting coordination with agencies such as the Treasury Department or U.S. Trade Representative.[111] Participation in these efforts remained voluntary, as senior officials acknowledged that exports to China and diaspora-driven sister cities, amongst other issues, were very important to local communities.[112] A senior State Department official noted that the weekly questions from local officials were just "the tip of the iceberg" and were likely to increase as China "doubles down."[113]

Under the second Trump administration, federal policy has continued to emphasize heightened scrutiny of PRC outreach, while many Republican members of Congress have publicly and privately pressured city leaders to curtail relationships with China. For example, House Republicans introduced

the Washington Sister Cities Act to prohibit the District of Columbia from maintaining sister-city ties with cities in China, and Republican members of the China Select Committee sent letters to U.S. mayors detailing their concerns over diplomatic relationships with Beijing.[114] Given these strong anti-China sentiments, experts in U.S.-China subnational relations expect that city officials will be very reluctant to share any information about requested meetings or partnerships from Chinese officials that could be in their community's interests. Sharing information could make them susceptible to retribution from federal politicians such as Representative Jim Banks (R-IN), who publicly lambasted the mayor of Carmel for traveling to China and signing a sister city agreement.[115] The result will likely be increased Chinese solicitation alongside decreased support and oversight from the federal government.

The juxtaposition of geopolitical tensions between the U.S. and China alongside political tensions between the U.S. executive branch and municipal governments creates vulnerability in U.S. international security. The National Counterintelligence and Security Center's 2022 report called on local leaders to "maintain enduring connectivity with U.S. authorities," yet these communication channels are being eroded by politicized federal actions. U.S.-China experts Kyle Jaros and Sara Newland find that this situation creates a risk that the PRC will "seek to exploit strains between cities and the federal government to gain diplomatic leverage" by establishing in-roads with local governments isolated from federal support.[116]

The lack of coordination hinders U.S. mayors from accessing information necessary to engage in symmetric relationships. Mayoral offices typically lack the intelligence and resources to draw the line between transparent and nefarious engagement. Federal agencies have the ability to provide this information: FBI field offices can provide data on local organizations with suspected ties to the united front and CCP, the USTR can review proposed language for trade-focused MOUs, and the State Department can brief local officials on security risks and country trends ahead of foreign trips.

The lack of coordination additionally prevents the federal government from understanding a key foreign policy strategy of a foreign country. Additionally, regular communication with local officials can help the FBI identify trends with

immense national security implications, such as the types of dominant industries in cities being solicited by China or requested priorities for MOUs.

Reciprocal and transparent city-to-city communication channels are valuable tools for many U.S. mayors, especially as national-level U.S.-China relations remain tense and unpredictable. The Berkeley-China Climate Subnational program is a prime example, as it enables cooperation on issues such as greenhouse gas and air pollution reduction and clean energy development between major urban emitters, including Beijing, Chongqing, Hong Kong, Suzhou in China and Los Angeles and San Francisco in the United States—cities whose climate policies have outsized global impact. Nearly two months into the reciprocal tariff escalation between the U.S. and China, leaders from the Port of Long Beach, the Port of Los Angeles, and the Port of Shanghai convened to continue progress on the two-year Green Shipping Corridor agreement with the goal of zero lifecycle carbon container ships on the corridor by 2030.[117]

For mayors whose cities have significant Chinese diaspora communities, longstanding cultural partnerships with Chinese cities, or economic interests tied to Chinese markets, severing ties is neither feasible nor desirable, even amid ongoing tariffs and trade restrictions.

To sustain the advantages of international partnerships while avoiding security risks, U.S. mayors should be equipped with federal guidance and consistent support mechanisms. China's strategic emphasis on empowering local governments to advance its foreign policy objectives underscores a gap in the U.S. approach. **The United States would benefit from a more nuanced and pragmatic approach to Chinese engagement that facilitates practical, community-to-community relationships led by local government leaders, while also managing broad, strategic considerations at the national level.**

Cross-Cutting Case Studies

The following section examines the interplay between these issues in practice by exploring the approach of four cities between 2015-2025.

New York City

As a city constantly in the global spotlight, New York City has spearheaded an international security approach that, while coordinated among actors, remains fragmented across specific issues.

The city stands out for leadership in cybersecurity: the industry-leading NYC Cyber Command was created in 2017 with the goal of being "the most cyber resilient city in the world" and has been referred to as the "gold standard for a city approach" by the Global Cyber Alliance.[118] The city's proactive stance is enabled by robust state policies that prioritize cyber hygiene. In 2022, Governor Kathy Hochul announced a Joint Security Operations Center that enables real-time intelligence sharing and collaboration between local, state, and federal cyber defenders. In June 2025, Governor Kathy Hochul signed legislation aimed at "enhancing the cybersecurity and resilience of state and local government networks across New York" with policy measures including mandatory reporting of cyber incidents within 72 hours and annual cybersecurity training.[119] These policies contribute to an ecosystem in which "[what] New York, with the federal government, with the New York Field Office of the FBI, really pioneered after 9/11 is that we're all on the same team."

New York City not only stands out for its approach to cybersecurity, but also in its approach to drug trafficking and TCOs. The New York Police Department (NYPD) leads enforcement against drug trafficking networks and collaborates with federal and statewide task forces, while the Office of the Special Narcotics Prosecutor (SNP) is a unique, independent agency that coordinates high-profile prosecutions involving national and international organizations. SNP, the only agency of its kind in the United States, was established in response to the city's role as a destination of international narcotics and is equipped to proactively investigate TCOs using international legal frameworks. Federal and state agencies, including DEA and HSI, can bring cases to SNP. While the NYC mayor has an Office of Criminal Justice to provide policy-level support, operational coordination with federal agencies is primarily led by liaisons within SNP and NYPD.

While intergovernmental cooperation has been managed in a structured manner largely independent from the city government, recent moves to bring greater federal oversight have sparked controversy. In April 2025, Mayor Eric Adams allowed ICE to open an office at Rikers jail due to the presence of "violent transnational gangs and criminal enterprises... that have been designated by federal authorities as foreign terrorist organizations."[120] The City Council subsequently sued to block Mayor Adams' executive order, arguing it blocked the city's 2014 sanctuary restrictions on ICE at Rikers and was tainted by an apparent quid pro quo deal with the Trump Administration tied to his own legal challenges. The City Council argued that ICE was banned from Rikers since 2014 under sanctuary laws that are still in effect, and in September 2025 the New York State Supreme Court declared the executive order null and void.[121]

While NYC has developed a structured approach to cybersecurity and transnational gang enforcement, several high-profile investigations involving suspected agents of the PRC both within and outside of local government offices have raised alarm about the scope and methods of foreign influence efforts. Linda Sun, the Former Deputy Chief of Staff to Governor Kathy Hochul, was accused of acting as an undisclosed agent of the PRC in 2024, including allegedly blocking Taiwanese representatives from meeting with the governor. Sun's federal trial ended in a mistrial due to a hung jury, and prosecutors have indicated their intent to retry the case. Separately, Mayor Eric Adams' former advisor and fundraiser, Winnie Greco, has been under FBI investigation since 2024 for suspected conspiracy charges, but has not been publicly charged as of 2026.[122]

In separate cases outside of local government, Manhattan resident Chen Jinping, a U.S. citizen, pleaded guilty in December 2024 to conspiring to act as an agent of the PRC and operating an undeclared "overseas police station" in Lower Manhattan for China's Ministry of Public Security. DOJ officials characterized the operation as a "a clear affront to American sovereignty and danger to our community."[123] Separately, Yuanjun Tang, a naturalized U.S. citizen and former dissident based in Queens, pleaded guilty in September 2025 to conspiring to act as an unregistered agent of the PRC by gathering information on U.S.-based Chinese pro-democracy activists and reporting it to the PRC's Ministry of State Security.[124]

Houston

As a major hub for critical infrastructure, including the Port of Houston and two major airports, Houston is a prominent target for cyberattacks. These risks have prompted a comprehensive response. Oversight is primarily provided by the Houston Police Department, which leads investigations into cyber and financial crimes through task force models in partnership with the FBI and the U.S. Secret Service.[125] Established in 2018, the Cyber & Financial Crimes Division is tasked with addressing offenses at the local, national, and international levels.[126] Although documented threats[127] exist to Houston's energy, aviation, and health care sectors, in addition to airports, the city has not publicized any news of international attacks. The only high-profile case in the area, a Chinese-suspected attack on the Port of Houston, was blocked by the Port Authority, which held jurisdiction over the issue.[128]

Like in New York, local government staffers with relevant responsibilities are required to conduct annual cybersecurity trainings, but the quality of the training varies across jurisdictions. The Texas Department of Information Resources certifies a pool of eligible trainings, and some municipalities opt for minimal options, such as a 19-minute YouTube video and self-administered test - with an answer key.[129] Municipalities have fewer resources at their disposal to complement these trainings; while the nonprofit Texas Municipal League (TML) provides a cybersecurity clearinghouse and resources for all Texas cities, 30% of the links on their website were broken or went to the wrong site and 60% were from 2016 or earlier.[130]

Houston is a critical hub for drug trafficking and TCO presence in the United States and therefore has substantial federal involvement in policies impacting the metropolitan area. The Houston High Intensity Drug Trafficking Area (HIDTA), which was federally designated in 1990, now covers 18 counties and is recognized as one of the most significant distribution and transshipment areas for trafficked illicit drugs entering from Mexico.[131] HIDTA operations coordinate federal task forces and local law enforcement and, while Houston Police Department assigns officers to task forces and can join the executive board, the city government does not have influence over the operations. Unlike New York, where prosecution is centralized under the Special Narcotics Prosecutor, drug trafficking cases in Houston are handled either by the District Attorney's Office or U.S. Attorney's Office. Houston is also home to a fusion center, the Houston Police Department-led Houston Regional Intelligence Service Center, which has focused on gathering counter-terrorism criminal intelligence to identify threats.[132]

Houston was the setting for a major escalation in the national U.S.-China relationship in 2020, when the U.S. closed the Chinese consulate in Houston. The State Department's accusations included use of false identification, illegal transfer of sensitive information, plans to recruit researchers and academics from Houston to Chinese institutions, and coercion of Chinese citizens in the U.S. under surveillance from China.[133] Then-Senator Marco Rubio referred to the consulate as "the central node of the Communist Party's vast network of spies and influence operations in the United States."[134] While the consulate is governed by national policies, the closure had implications for students in Houston schools, potential Chinese energy and petrochemicals investments, and xenophobic incidents. Despite this, Mayor Sylvester Turner was not notified ahead of the decision, putting him in a reactive position of discouraging any resulting anti-China sentiments and expressing hopes for continued cooperation with China on COVID-19 personal protective equipment.[135]

Des Moines

Des Moines, while a smaller population than Houston, New York City, or San Francisco and lacking their globally critical infrastructure, has nevertheless faced substantial cybersecurity challenges. The special agent in charge of the FBI Omaha Field Office, which oversees operations in Nebraska and Iowa, noted in 2022 that "The cyber threat to our businesses, farms, food processing facilities, local governments, and communities in Iowa is increasing exponentially"[136] The most high-profile attack occurred against the Des Moines public school system in 2023, when the whole system was taken offline in a ransomware attack.

The Iowa Cyber Resilience Initiative exemplifies the potential of academic-local government partnerships with federal support. In FY 2022, Iowa State University stepped up to lead the Iowa Cyber Resilience Initiative, funded by the DHS State and Local Cybersecurity Grant Program. This initiative kicked off in October 2025 with a State Cybersecurity Conference that provided trainings for officials from Iowa's counties, cities, and schools.[137]

As cybersecurity risks increase nationwide, Des Moines possesses several attributes that could make it more vulnerable. In recent years, the city has become an emerging hub for data centers, including Microsoft and Meta, which could put their cyber responses under increased pressure. Additionally, as national support for election-related cybersecurity responses is rolled back, Iowa's role as the first GOP caucus could make it a target for foreign interference.

Iowa's economic conditions have historically promoted pragmatic cooperation between city officials and China. Iowa represents approximately 50% of U.S. soybean exports, and China has been the dominant importer for the past two decades. However, Iowa State University reports that reciprocal tariffs could cost the Iowa soybean industry between $191 million and $1.49 billion.[138] The Kimberleys, who own a farm 30 minutes from Des Moines and have hosted Chinese delegations, epitomize the impact of these economic ties: "With China being the largest buyer of U.S. soybeans, we have to realize we don't have much control over the political scene, but if we can work with people to help our industry, that is what we are going to do."[139]

During a Des Moines event in 2023 where U.S. and Chinese companies signed soybean purchasing agreements, the president emeritus of the World Food Prize Foundation encouraged the audience to "just remember these three words: Peace through agriculture." This sentiment was echoed by Chinese ambassador to the U.S. Xie Feng, who claimed that "We strive to maintain this stable and mutually beneficial collaboration between China and U.S. soy as the ballast for successful bilateral economic and trade relations."[140]

Even deep-seated economic ties may not be capable of weathering CCP's escalating tactics and U.S. anti-China sentiment. In August 2025, Congressman John Moolenaar, the same who brought national attention to the Gotion plant, wrote a fiery letter to Mayor Connie Boesen of Des Moines calling on her to end the sister city relationship with Shijiazhuang City and "cease all future engagements with CPAFFC."[141] This was provoked by a local high school gospel choir's trip to China in July, sponsored by the PRC government. Congressman Moolenaar claimed to possess intelligence that students were required students to download WeChat, and he argued that "American youth groups should not be used as propaganda tools of the Chinese government." The City of Des Moines later responded that

they had no oversight of the trip in question, which was facilitated by a community group.[142]

Des Moines is primarily a consumer drug market yet has also become a secondary distribution hub for drugs arriving from Chicago and Mexico. Drug trafficking responses are typically managed through regional initiatives; Des Moines participates in the Midwest HIDTA network through the DEA's Des Moines Task Force, which coordinates with local law enforcement on interdiction, intelligence sharing, and arrests. Des Moines is also home to the State of Iowa Intelligence Fusion Center which coordinates with statewide drug task forces. In May 2023, the DEA concluded the one-year "Operation Last Mile," which arrested 29 Iowans for dealing fentanyl and methamphetamine in coordination with the Mexican-based Sinaloa and Jalisco Cartels.[143] The city's integration into this federal framework highlights how Des Moines's drug policy operates through shared jurisdiction mechanisms, illustrating the dependence of mid-sized municipalities on federal task forces and the growing regionalization of responses to transnational criminal activity.

San Francisco

Since 2007, San Franciso has been home to the Northern California Regional Intelligence Center (NCRIC), a fusion center that aims to support critical infrastructure and cybersecurity protection through partnerships with the private sector. In 2021, San Fransico institutionalized the centralized Office of Cyber Security in the city charter. Chief Information Officer Michael Makstman describes this as a unique approach across large U.S. cities that aims to improve coordination across government offices. In 2023, Makstman described a "tsunami" of cybercrime, estimated at a 30% increase in cyberattacks between 2020 and 2023.[144] One of the most high-profile attacks occurred in January 2023, when the Vice Society ransomware group stole more than 120,000 internal law enforcement records from San Francisco's Bay Area Rapid Transit (BART).[145] Later that year, San Francisco held the first citywide cyber exercise with both traditional IT and cyber teams and the Department of Emergency Management.[146]

During his tenure, CIO Makstman has prioritized engagement with other U.S. cities by serving as Co-Chair of the Coalition of City Chief Information Security Officers. While the coalition largely relies on informal information sharing and

communication, there remains a need for institutionalized agreements in times of emergency, and they are exploring partnership models with the National League of Cities and U.S. Conference of Mayors.[147]

San Francisco, like Des Moines, has deep economic ties with China that provided a base of cooperation during both Biden and Trump administrations. However, the coordination with the national government has varied. Between 2023 and 2024, city and state level officials maintained close communication with the Biden administration as they hosted official delegations, such as Xi Jinping's visit for APEC.[148] Later that year, governors of California and the Guangdong province and officials from five cities and four provinces of China gathered in nearby Berkeley to discuss subnational climate cooperation; in particular, the two regions signed an MOU to explore a joint agenda on carbon-market development and climate finance.[149] However, in February 2025, an anonymous city government official in California noted that "The fact that we would love to see Chinese money coming into San Francisco is contrary to what they are doing in Washington right now. Washington is 4500 km away. We're a Pacific city. The ties with China are incredibly important to the success of this city."[150]

In 2024, Mayor London Breed made a multi-city trip to China that spotlighted the political complexities of U.S.-China subnational relationships. The trip aimed to boost tourism, notably through the request of two pandas, and was organized by the CPAFFC. Although Mayor Breed received a State Department briefing before the trip, national media concentrated on the lack of a C.I.A briefing on "counterintelligence threats she might face in China and how officials there might try to manipulate her."[151] Breed's trip also occurred ahead of a competitive mayoral election, which some U.S.–China scholars argued left her politically vulnerable, suggesting she "ceded political leverage to Chinese government actors rather than approaching city diplomacy from a position of maximum strength."[152]

San Francisco has experienced dramatic shifts in their federal collaboration on drug trafficking in recent years. In 2023, the mayor co-sponsored a U.S. Conference of Mayors resolution noting that "local efforts are currently outmatched by the scale of the current international, organized crime operations that are funneling fentanyl into our communities."[153] The resolution called on the federal government to expand their engagement with local law enforcement with

a particular mention of joint investigations, which have indeed increased since 2023.

However, this relationship was jeopardized in October 2025, when the Trump Administration announced a major "surge" of National Guard and ICE agents to detect undocumented immigrants and "narco-terrorists."[154] This prompted protests and alarm from local government officials. Mayor Lurie argued that continued support with DEA was welcome, but "sending them [the National Guard] to San Francisco will do nothing to get fentanyl off the streets or make our city safer."[155] The CEOs of Nvidia and Salesforce then echoed the mayor's request for a reduction of federal interference in a private call with President Trump. The combined efforts worked, and he called off the national operation on October 24.

Recommendations

These interlinking security challenges can be most effectively addressed by an integrated international security response. The following recommendations outline key steps that both the federal government and municipal governments can take to empower mayors to continue pursuing their diplomatic engagement with stronger frameworks for managing international security risks in place.

Recommendations for national leaders to support subnational security efforts:

1. **Formalize Federal-Local Communication Protocols for National Security Threats:** Offices of intergovernmental affairs at relevant federal agencies (including DOD, DOJ, and DHS) should establish standardized protocols for confidentially alerting city mayors and governors of credible, significant international security risks in their jurisdiction, such as suspected foreign espionage, cyber operations, or transnational criminal organization (TCO) activity. Timely notification would ensure that municipal leaders are included in early decision-making, equipped to coordinate with federal partners, and able to prepare risk communication for their communities before details become public. Models for such information sharing between law enforcement agencies already exist for certain threats via fusion centers and federal bulletins, but these frameworks do not consistently guarantee direct, advance notification to local government officials. Institutionalizing this practice would address the persistent gap that leaves local leaders learning about threats from news reports or after federal action is underway, which puts them in a reactive position that undermines their credibility to support their constituents and engage internationally.

2. **Integrate Municipal Priorities into Local-Federal Law Enforcement Partnerships:** Mayors, as elected officials, are accountable to their constituents and must balance public safety with local values and priorities. The task force model employed by various federal agencies prioritizes coordination among law enforcement agencies, often leaving mayors without a voice in operational decision-making. This top-down approach can risk alienating key communities if federal priorities diverge from local needs. To facilitate more sustainable agreements, federal task forces should consider creating formal mechanisms for municipal governments to provide input on partnership priorities. A more collaborative approach from policy creation may reduce the likelihood that local government officials feel compelled to fully accept or reject participation and information sharing.

3. **Institutionalize Municipal Government Representation in Fusion Centers:** The National Fusion Center Association should consider prioritizing input from local elected officials and community organizations, in addition to law enforcement agencies, when collaborating with federal partners to develop nationwide fusion center performance metrics and update SAR indicators, to ensure that centers address practical national security challenges and are grounded in reciprocal, trust-based relationships with local stakeholders. When establishing new urban fusion centers, the State Homeland Security Advisor should ensure consistent engagement with city administration, even though formal approval is not required. Fusion center directors should also seek to gain local government representation in the Fusion Center Liaison program, rather than limiting it to law enforcement and related personnel.

4. **Publish Guideline Database for Subnational Engagement with China:** A nonpartisan organization should publish a database including an outreach protocol, clear legal parameters for engagement, informational overviews of the party-state governance system and subnational oversight agencies, sample MOU templates, and "hotline" connections to relevant agencies (including USTR and FBI) that mayoral offices can turn to for specific questions, with input from the Office of the Director of National Intelligence and Department of State. This approach will allow mayors to engage responsibly with Chinese officials and balances the objective of providing federal guidance while not restricting U.S. mayors' autonomy. Publishing guidelines also reduces the administrative burden on State Department officials to answer consistent questions. This recommendation builds upon recently published guidance for engaging with China prepared by ALLIES (Alliance for Local Leaders International)[156] as well as recommendations from the Truman Center to create institutionalized platforms for knowledge-sharing among cities, and between cities and the federal government.[157]

5. **Pilot a Federal-Local Security Fellowship:** A fellowship specifically focused on connecting federal international security officials without embedding intelligence or investigative functions at the municipal level would kickstart risk response protocols in underprepared cities and enhance existing processes in more advanced cities, while also providing enduring connections between

local and federal government offices. This fellowship could place experienced federal policy professionals into temporary advisory roles, building on the model of previous initiatives such as the Lewis Local Diplomat and Pearson Fellowship, which connected foreign service officers from the U.S. Department of State to local governments and congressional offices. Fellows could clarify legal and procedural pathways and facilitate referrals to federal agencies when issues arise. The voluntary application process for cities could allow for a targeted approach, as cities with particularly active security threats could request support from a federal officer in a specific agency with relevant expertise.

Recommendations for municipal leaders to expand security efforts:

1. **Convene a Municipal National Security Commission:** A standing commission made up of representatives from offices of international affairs or trade, public safety and emergency management, and cybersecurity can enhance horizontal cooperation across city agencies. The commission can also improve vertical coordination by serving as the primary body liaising with state and federal security agencies. This commission could be responsible for tracking and maintaining communication with international and domestic partners to ensure greater continuity between shifting administrations, as well as engaging with diaspora communities. This commission will strengthen the work of its component offices by ensuring the consideration of security implications of economic, cultural, and technological policies. The initial task of the commission can be developing a municipal national security framework with guidelines for responding to risks that draws from established national guidelines but is tailored to address the unique attributes and needs of the city.

2. **Establish National Security Task Force within the U.S. Conference of Mayors (USCM):** As a mayor-led, third-party organization, the USCM is an excellent platform for developing security and risk analysis solutions that can be scaled across cities. The Conference could use their agenda-setting power to demonstrate the urgency of creating city plans to address cybersecurity, drug trafficking, and adversarial foreign interference at a local level, while also using their network to invite speakers for targeted briefings. This Task Force could identify priorities such as creating a transparent and permanent registry of all new U.S.-China agreements that would allow mayors to watch for emerging trends in Chinese engagement and examine strategies

for reciprocal relationships that have brought shared benefits. Since USCM task forces develop Conference policy positions, a new task force could synthesize nationwide subnational threats into more coherent and actionable recommendations for local and federal government responses.

3. **Create Repository for Non-Sensitive Municipal Cybersecurity Code:** Given inconsistencies in federal funding, U.S. cities should jointly lower the costs and strengthen the effectiveness of cyber defenses by developing secure repository platforms dedicated to the sharing of non-sensitive, non-operational code, infrastructure automation templates, and general cyber hygiene best practices. While MS-ISAC provides state and local governments with indicators of compromise and detection signatures, this proposed repository focuses on sharing preventative infrastructure and practices. As modeled by NYC Cyber Command, municipalities across the country can build security infrastructure using open-source tools and infrastructure as code frameworks.

4. **Build Community Advisory Councils:** City governments can benefit from the national security expertise of local universities, the risk analysis capacities of private companies, and the intercultural knowledge of diaspora communities.158 An advisory council made up of community experts on different security issue areas could be consulted in the development of security protocols and ahead of key decisions, such as a trade-focused MOU with Taiwan, an all-expenses paid class trip to Shanghai, or major TCO arrests in a neighboring town. These councils should seek to achieve diverse perspectives within all sectors to ensure that no single perspective or cultural background is monopolizing policy.

5. **Institutionalize a Whole-of-State Approach to Cybersecurity:** City governments should collaborate with their state government through cybersecurity planning committees, as required by the SLCGP, with equal participation from state, local, and business community leaders. This standing cooperation is essential for navigating emerging challenges in cybersecurity, such as AI. Because private companies are frequently targeted, there must be clear communication pathways to local officials. Coordinated efforts should include comprehensive risk assessments and targeted resources, such as free annual cybersecurity training, provided in high-risk areas. These committees should ground their activities in a municipal cyber assessment.

Conclusion

All three of these challenges have been traditionally conceived solely within the purview of the national government, yet current threat assessments reveal the limitations of this approach. Mayors are aware of these challenges and are taking proactive, often coordinated, steps to address them without consistent federal support. Yet, this should be a priority at the national level, as well. **Subnational security policies should be a core component of every city's international playbook, while municipal engagement should be prioritized in every national government threat assessment and security strategy.**

Each security issue provides a greater test for U.S. federalism. The city-state-federal model has the potential to provide mayors with informed agility to conduct international relationships that benefit their communities while remaining alert to potential risks. However, the model is falling short. While federal agencies are directing ample resources and attention towards addressing drug trafficking and TCOs in cities, mayors typically lack political agency in the process and are raising concerns that federal focus on immigration enforcement is actually undermining these investigations. The circumstances reverse when it comes to cybersecurity policy, as mayors have been able to innovate and drive their own solutions yet lack resources to implement widespread security overhauls. Finally, the issue of PRC engagement shows the detriments of inconsistent federal policy, as mayors are disincentivized to seek federal support and coordination that would be beneficial for all levels of government.

The fusion center model illustrates the status quo approach to local-federal intelligence sharing, where federal agencies direct a flow of sanitized intelligence to local law enforcement, which in turn reports on designated threat indicators. Yet the police officers and detectives primarily engaged with federal law enforcement are rarely the officials responsible for approving foreign-owned factories or authorizing partnerships with private sector firms to implement advanced cybersecurity programs.

While mayors of large cities have addressed aspects of these issues for decades, the growing interdependence among them now requires a more integrated response. The 2024 and 2025 Intelligence Community Threat Assessment reports list China as one of the most active cyber threats to the U.S. government. In particular, China is developing targeted disinformation campaigns using AI. China has also been the primary source of illegal fentanyl since 2013 and only placed it on the list of controlled substances in 2019.

These challenges have common roots in foreign policy conflicts, and the U.S.-China standoff demonstrates how geopolitics is increasingly being played out at the local level. For foreign adversaries, targeting a large U.S. city's infrastructure or influencing local elections may be a strategic approach to gain influence without necessarily evoking a federal level response.

These issues can no longer be addressed in silos; the IT manager analyzing weaknesses in the energy grid should be talking to the international trade advisor working on a new U.S.-China MOU on trade, as well as the local police chief on the sourcing of key chemicals in new drugs. Assembling a comprehensive view and strategy of geopolitical risk and defense is an essential step in protecting mayors of large cities who are already active internationally. While the resources dedicated to this issue may be less for smaller and less internationally engaged cities, the cases in Gotion and Des Moines reveal the risks of not adopting a defense-oriented approach.

The balance of diplomacy, defense, and homeland security is taken as a given at the national level. It's time for city leaders - supported by federal guidance and sustained resources - to adopt a similarly integrated approach to build intentional and strategic international partnerships.

Endnotes

1 Cynthia Moreno, Khia Duncan, Dalia Gonzalez, et al., *State of Immigrants in Los Angeles County 2024*, Los Angeles: USC Equity Research Institute & California Community Foundation, July 11, 2024, https://dornsife.usc.edu/eri/wp-content/uploads/sites/41/2024/07/Final_SOILA2024_Full_Report_v3.pdf.

2 Jon Temin and Max Bouchet, "The United States Needs Subnational Diplomacy More Than Ever," *Foreign Policy*, October 25, 2024, https://foreignpolicy.com/2024/10/25/subnational-diplomacy-mayors-governors-united-states-climate/.

3 Lorenzo Kihlgren Grandi and Cecilia Emma Sottilotta, *When City Diplomacy Meets Geopolitics: A Framework to Help Cities Navigate Geopolitical Risk*, IFRI (French Institute of International Relations), February 27, 2025, https://www.ifri.org/en/memos/when-city-diplomacy-meets-geopolitics-framework-help-cities-navigate-geopolitical-risk.

4 Christopher Wray, "FBI Director Wray testifies in House hearing on Chinese cybersecurity threat to U.S.," *Rev*, January 31, 2024, https://www.rev.com/transcripts/fbi-director-wray-testifies-in-house-hearing-on-chinese-cybersecurity-threat-to-u-s-transcript.

5 Alexander Palmer, Riley McCabe, Daniel Byman, and Skyeler Jackson, *Global Terrorism Threat Assessment 2025, Center for Strategic and International Studies, March 28, 2025,* https://www.csis.org/analysis/global-terrorism-threat-assessment-2025.

6 "Homeland Security & Cybersecurity," *National Governors Association,* https://www.nga.org/bestpractices/homeland-security.

7 Jon Temin and Max Bouchet, "The United States Needs Subnational Diplomacy More Than Ever."

8 American Foreign Service Association, "Subnational Diplomacy: A Conversation with Special Representative Nina Hachigian," *Foreign Service Journal*, December 3, 2024, https://www.afsa.org/subnational-diplomacy-conversation-special-representative-nina-hachigian.

9 Stephen P. Mulligan, *Constitutional Limits on States' Power over Foreign Affairs*, Congressional Research Service, August 15, 2022, https://www.congress.gov/crs-product/LSB10808.

10 A full list of relevant agencies includes the Office of the Director of National Intelligence (ODNI), Department of Defense (DOD), Department of the Treasury (Treasury), Department of Commerce (DOC), United States Secret Service (USSS), Department of State (DOS), National Security Agency (NSA).

11 *Federal Support for and Involvement in State and Local Fusion Centers, U.S. Senate Permanent Subcommittee on Investigations,* October 3, 2012, https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/10-3-2012%20PSI%20STAFF%20REPORT%20re%20FUSION%20CENTERS.2.pdf.

12 Interview #16.

13 Interview #16.

14 Interview #16.

15 Interview #13.

16 Alexi Horowitz-Ghazi, "When Chinese Manufacturing Met Small Town, USA," *Planet Money* (NPR), June 6, 2025, https://www.npr.org/transcripts/1253756223.

17 Jon Paul Kemp, "Feds decline review of Chinese battery-plant plans in Big Rapids, company says," *Detroit News*, June 13, 2023, https://www.detroitnews.com/story/business/autos/2023/06/13/feds-decline-review-of-chinese-battery-plant-plans-in-big-rapids-company-says/70317340007/.

18 Christopher Wray, "FBI Director Wray testifies in House hearing on Chinese cybersecurity threat to U.S.," *Rev*, January 31, 2024, https://www.rev.com/transcripts/fbi-director-wray-testifies-in-house-hearing-on-chinese-cybersecurity-threat-to-u-s-transcript.

19 Jamie A. Hope, "Legislators ask state to send $275K to Green Township for its fight against Gotion," *Michigan Capitol Confidential*, May 30, 2025, https://www.michigancapitolconfidential.com/news/legislators-ask-state-to-send-275k-to-green-township-for-its-fight-against-gotion.

20 *Homeland Threat Assessment 2025*, U.S. Department of Homeland Security, September 30, 2024, https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf.

21 Interview #9.

22 Vanda Felbab-Brown, Jonathan P. Caulkins, Carol Graham, Keith Humphreys, Rosalie Liccardo Pacula, Bryce Pardo, Peter Reuter, Bradley D. Stein, and Paul H. Wise, *The Opioid Crisis in America: Domestic and International Dimensions*, Brookings Institution, June 2020, https://www.brookings.edu/wp-content/uploads/2020/06/0_Overview.pdf.

23 "The Expansion and Diversification of Mexican Cartels: Dynamic New Actors and Markets," International Institute for Strategic Studies (IISS), December 12, 2024, https://www.iiss.org/publications/armed-conflict-survey/2024/the-expansion-and-diversification-of-mexican-cartels-dynamic-new-actors-and-markets/.

24 *2025 Annual Threat Assessment of the U.S. Intelligence Community*, Office of the Director of National Intelligence.

25 *2024 Annual Threat Assessment of the U.S. Intelligence Community, Office of the Director of National Intelligence, March 11, 2024,* https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3787-2024-annual-threat-assessment-of-the-u-s-intelligence-community.

26 "Quick Facts on Fentanyl: FY 23," United States Sentencing Commission, https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Fentanyl_FY23.pdf.

27 *2025 National Drug Threat Assessment,* U.S. Drug Enforcement Administration, May 2025, https://www.dea.gov/documents/2025/2025-05/2025-05-13/national-drug-threat-assessment.

28 *National Firearms Commerce and Trafficking Assessment (NFCTA): Volume IV – Part VII, Firearm Commerce, Crime Guns, and the Southwest Border*, Bureau of Alcohol, Tobacco, Firearms and Explosives, January 8, 2025, https://www.atf.gov/firearms/docs/report/nfcta-volume-iv-part-vii-%E2%80%93-firearm-commerce-crime-guns-and-southwest-border/download.

29 Interview #11.

30 "High Intensity Drug Trafficking Areas (HIDTA) Program," U.S. Drug Enforcement Administration, https://www.dea.gov/operations/hidta.

31 "The Department of Justice Announces Takedown of Key MS-13 Criminal Leadership," U.S. Department of Justice, July 15, 2020, https://www.justice.gov/archives/opa/pr/department-justice-announces-takedown-key-ms-13-criminal-leadership.

32 "Sinaloa cartel leaders charged with narco-terrorism, material support of terrorism and drug trafficking," U.S. Immigration and Customs Enforcement, May 14, 2025, https://www.ice.gov/news/releases/sinaloa-cartel-leaders-charged-narco-terrorism-material-support-terrorism-and-drug.

33 "Reviving 287(g) Agreements Under the New Administration: Implementation, Concerns, and Implications," *National Immigration Forum Explainer*, April 28, 2025, https://www.immigrationforum.org/article/reviving-the-287g-agreements-under-the-new-administration-implementation-concerns-and-implications/.

34 Tom K. Wong, "How Interior Immigration Enforcement Affects Trust in Law Enforcement," US Immigration Policy Center, University of California San Diego, April 3, 2019, https://usipc.ucsd.edu/publications/usipc-working-paper-2.pdf.

35 "How Law Enforcement Can Better Engage Immigrant Communities: Promising Practices and Challenges from a National Survey and Regional Meetings," Police Executive Research Forum, June 2023, https://www.policeforum.org/assets/EngageImmigrantCommunities.pdf.

36 Danielle Scruggs, "Photos: Thousands Once Again Protest ICE in Minneapolis and Across the U.S.," *National Public Radio (NPR),* January 30, 2026, https://www.npr.org/sections/the-picture-show/2026/01/30/g-s1-108087/photos-thousands-once-again-protest-ice-in-minneapolis-and-across-the-u-s.

37 Jacob Frey, "The Interview: A Terrifying Line is Being Crossed," *The New York Times*, January 31, 2026, https://www.nytimes.com/2026/01/31/magazine/jacob-frey-interview.html.

38 "Statement from the U.S. Conference of Mayors Following Death of Another Protestor in Minneapolis," The United States Conference of Mayors, January 24, 2026, https://www.usmayors.org/2026/01/24/statement-from-the-u-s-conference-of-mayors-following-death-of-another-protestor-in-minneapolis/.

39 Jacob Frey, "The Interview: A Terrifying Line is Being Crossed"

40 "What to Know About the Homeland Security Shutdown," *The New York Times,* February 15, 2026.

41 Megan Cassidy and Gabrielle Lurie, "This Is the Hometown of San Francisco's Drug Dealers," *San Francisco Chronicle,* September 27, 2024, https://www.sfchronicle.com/projects/2023/san-francisco-drug-trade-honduras/.

42 Eve Zuckoff, "At Annual Conference, Republican Mayors Call for De-escalation in Minnesota," *National Public Radio (NPR),* January 29, 2026, https://www.npr.org/2026/01/29/nx-s1-5691818/at-annual-conference-republican-mayors-call-for-de-escalation-in-minnesota.

43 "Balancing community trust and enforcement: The complex issue of immigration," Police Executive Research Forum, April 12, 2025, https://www.policeforum.org/trending12apr25.

44 Ximena Bustillo, "Homeland Security pulls down list of 'sanctuary' cities and counties after backlash," *National Public Radio (NPR),* June 2, 2025, https://www.npr.org/2025/06/02/nx-s1-5421232/homeland-security-sanctuary-cities-immigration.

45 Interview #11.

46 "Republicans target Nashville's mayor for his response to immigration arrests," *Associated Press,* June 3, 2025, https://www.apnews.com/article/d5af5390fd4858a4c570e49cf3be7722.

47 Jacob Frey, "The Interview: A Terrifying Line is Being Crossed," *The New York Times*, January 31, 2026, https://www.nytimes.com/2026/01/31/magazine/jacob-frey-interview.html.

48 Eileen Sullivan and Zolan Kanno-Youngs, "D.H.S. Agents Reassigned Amid Internal Disputes Over Border Enforcement," *New York Times*, November 16, 2025, https://www.nytimes.com/2025/11/16/us/politics/dhs-agents-reassigned.html.

49 "First Binational Summit: U.S. – México Border Mayors Association," U.S. – México Border Mayors Association, August 16, 2011, https://usmex.ucsd.edu/_files/1st_summit.pdf.

50 "First Binational Summit: U.S. – México Border Mayors Association," U.S. – México Border Mayors Association.

51 Interview #9.

52 Christopher Wray, "FBI Director Wray testifies in House hearing on Chinese cybersecurity threat to U.S.," *Rev*, January 31, 2024, https://www.rev.com/transcripts/fbi-director-wray-testifies-in-house-hearing-on-chinese-cybersecurity-threat-to-u-s-transcript.

53 Jonathan Greig, "Attempted hack on NYC continues wave of cyberattacks against municipal governments," *The Record from Recorded Future News,* April 5, 2024, https://therecord.media/new-york-city-government-smishing-attack.

54 "Three Takeaways for Municipal Bond Issuers From the New SEC Cybersecurity Disclosure Rules," *McGuireWoods LLP*, September 6, 2023, https://www.mcguirewoods.com/client-resources/alerts/2023/9/three-takeaways-municipal-bond-issuers-new-sec-cybersecurity-disclosure-rules/.

55 Interview #10.

56 "The State of Ransomware 2025," *Sophos*, June 2025, https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf.

57 *2025 Annual Threat Assessment of the U.S. Intelligence Community*, Office of the Director of National Intelligence.

58 "The State of Ransomware in State and Local Government — 2024," *Sophos,* August 14, 2024, https://news.sophos.com/en-us/2024/08/14/the-state-of-ransomware-in-state-and-local-government-2024/.
"The State of Ransomware in State and Local Government — 2023," *Sophos*, August 1, 2023, https://news.sophos.com/en-us/2023/08/01/the-state-of-ransomware-in-state-and-local-government-2023/.

59 Interview #10.

60 "U.S. Environmental Protection Agency," *Cybersecurity Alert: Cityworks Vulnerability and Mitigations*, February 10, 2025, https://www.epa.gov/system/files/documents/2025-02/epa-ow-cybersecurity-alert_cityworks_2_10_2025_508c.pdf.

61 Eventus Security Advisory Team, "Cityworks Vulnerability Allows Attackers to Compromise Critical Infrastructure Systems," *Eventus Security Advisory,* https://advisory.eventussecurity.com/advisory/cityworks-vulnerability-allows-attackers-to-compromise-critical-infrastructure-systems/.

Dan Goodin, "Beijing may have breached U.S. government systems before Cityworks plugged a critical flaw," *CSO Online*, April 17, 2024, https://www.csoonline.com/article/3994082/beijing-may-have-breached-us-government-systems-before-cityworks-plugged-a-critical-flaw.html.

62 Ionut Arghire, "Cityworks Zero-Day Exploited by Chinese Hackers in U.S. Local Government Attacks," *SecurityWeek*, May 23, 2025, https://www.securityweek.com/cityworks-zero-day-exploited-by-chinese-hackers-in-us-local-government-attacks/.

Sergiu Gatlan, "Chinese Hackers Breach U.S. Local Governments Using Cityworks Zero-Day," *BleepingComputer*, May 22, 2025, https://www.bleepingcomputer.com/news/security/chinese-hackers-breach-us-local-governments-using-cityworks-zero-day/

63 "2020 Unit 42 IoT Threat Report," *Unit 42 by Palo Alto Networks, 2020,* https://unit42.paloaltonetworks.com/iot-threat-report-2020/.

64 Megan De Mar, "Vallas campaign condemns deepfake video posted to Twitter," *CBS Chicago*, February 27, 2023, https://www.cbsnews.com/chicago/news/vallas-campaign-deepfake-video/.

65 Shlomit Wagman and Sarah Hubbard, "Weaponized AI: A New Era of Threats and How We Can Counter It," *Harvard Kennedy School Ash Center for Democratic Governance and Innovation,* April 8, 2025, https://ash.harvard.edu/articles/weaponized-ai-a-new-era-of-threats/.

66 "Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets," Cybersecurity and Infrastructure Security Agency, December 1, 2020. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-296a.

67 Sean Lyngaas, "Iranian hackers probed election-related websites in 10 states, U.S. officials say," *CyberScoop*, October 30, 2020, https://cyberscoop.com/iran-election-hacking-state-websites-probe-fbi/.

68 Interview #1.

69 "Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations," Cybersecurity and Infrastructure Security Agency, August 28, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-241a.

70 Seth G. Jones, *Russia's Shadow War Against the West, Center for Strategic and International Studies (CSIS),* March 18, 2025, https://www.csis.org/analysis/russias-shadow-war-against-west.

71 Interview #1.

72 Interview #1.

73 Christopher Wray, "FBI Director Wray testifies in House hearing on Chinese cybersecurity threat to U.S.," *Rev*, January 31, 2024, https://www.rev.com/transcripts/fbi-director-wray-testifies-in-house-hearing-on-chinese-cybersecurity-threat-to-u-s-transcript.

74 Eric Geller, "U.S.: Russian hackers targeting state, local governments on eve of election," *Politico*, October 22, 2020, https://www.politico.com/news/2020/10/22/russian-hackers-state-local-governments-431327.

75 Donald F. Norris, Laura Mateczun, Anupam Joshi, and Tim Finin, "Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity," *Public Administration Review*, February 21, 2019, DOI: 10.1111/puar.13028.

76 "Federal Cybersecurity: America's Data at Risk," U.S. Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, June 25, 2019, https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2019-06-25%20PSI%20Staff%20Report%20-%20Federal%20Cybersecurity%20Updated.pdf.

77 "Miller-Meeks asks if feds are prepared to support states, cities fight cyber attacks," Office of Representative Mariannette Miller-Meeks, February 10, 2021, https://millermeeks.house.gov/media/in-the-news/miller-meeks-asks-if-feds-are-prepared-support-states-cities-fight-cyber-attacks.

78 "Testimony Before the House Committee on Homeland Security," U.S. House of Representatives, Committee on Homeland Security, April 1, 2025, https://homeland.house.gov/wp-content/uploads/2025/03/2025-04-01-CIP-HRG-Testimony.pdf.

79 "How Local Governments Can Use the Updated Federal Uniform Grants Guidance to Support Evidence-Based Policy and Spending," *Results for America*, October 2024. https://results4america.org/wp-content/uploads/2024/10/RFA-Local-Leverage-the-Federal-Uniform-Grants.pdf.

80 David E. Sanger and Nick Corasaniti, "Trump weakens U.S. cyberdefenses at a moment of rising danger," *The New York Times*, April 5, 2025, https://www.nytimes.com/2025/04/05/us/politics/trump-loomer-haugh-cyberattacks-elections.html.

81 "Local Cybersecurity Grant Program," Grants.gov, https://www.grants.gov/search-results-detail/360215.

82 David E. Sanger and Nick Corasaniti, "Trump weakens U.S. cyberdefenses at a moment of rising danger."

83 "Center for Internet Security facing federal funding cuts," *News10 ABC,* https://www.news10.com/top-stories/center-for-internet-security-facing-federal-funding-cuts/.

84 Christopher Wray, "FBI Director Wray testifies in House hearing on Chinese cybersecurity threat to U.S.," *Rev,* January 31, 2024, https://www.rev.com/transcripts/fbi-director-wray-testifies-in-house-hearing-on-chinese-cybersecurity-threat-to-u-s-transcript.

85 Jon Kamp, "U.S. mayors unite against paying ransom to hackers," *The Wall Street Journal,* July 10, 2019, https://www.wsj.com/articles/u-s-mayors-unite-against-paying-ransom-to-hackers-11562774950.

86 Colin Wood, "Governors, mayors, CIOs sign letter supporting state and local cyber grant reauthorization," *StateScoop*, September 18, 2025, https://statescoop.com/governors-mayors-cios-sign-letter-supporting-state-and-local-cyber-grant-reauthorization/.

87 Kyle A. Jaros and Sara A. Newland*, Bridges or Battlegrounds? American Cities in a Changing US-China Relationship,* Truman Center for National Policy, https://cdn.prod.website-files.com/60b7dbd50474251a2b8c4fc0/67bf8b376552dcd2acea22c2_TrumanCenter-USChina_5.pdf.

88 *Homeland Threat Assessment 2025,* U.S. Department of Homeland Security.

89 *2023 Annual Threat Assessment of the U.S. Intelligence Community,* Office of the Director of National Intelligence, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

90 "Safeguarding Our Future: Protecting Government and Business Leaders at the U.S. State and Local Level from People's Republic of China (PRC) Influence Operations," National Counterintelligence and Security Center, Office of the Director of National Intelligence, July 6, 2022, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/PRC_Subnational_Influence-06-July-2022.pdf.

91 Paul Costello and Mareike Ohlberg, "Cities Need to Talk About China," *German Marshall Fund of the United States*, May 5, 2021, https://www.gmfus.org/news/cities-need-talk-about-china.

92 Huizhong Wu, "How China used a mid-level government aide in New York to influence U.S. politics," *PBS NewsHour*, September 5, 2024, https://www.pbs.org/newshour/nation/how-china-used-a-mid-level-government-aide-in-new-york-to-influence-u-s-politics.

93 *China's Overseas United Front Work Background and Implications for the United States, U.S.-China Economic and Security Review Commission,* August 24, 2018, https://www.uscc.gov/research/chinas-overseas-united-front-work-background-and-implications-united-states.

94 Jessica Brandt, Normal Eisen, and Audrye Wong, "The Future of Democracy, Election Interference and Foreign Influence: What's at Stake?" *Council on Foreign Relations YouTube channel,* February 20, 2025, https://www.youtube.com/watch?v=vEj8csfVpN0.

95 Tracy Liu, "China Rekindles Sister City Ties as Relations Remain Strained," *VOA News,* February 16, 2024, https://www.voanews.com/a/china-rekindles-sister-city-ties-as-relations-remain-strained-/7491035.html.

96 Interview #5.

97 Interview #5.

98 Jessica Brandt, Normal Eisen, and Audrye Wong, "The Future of Democracy, Election Interference and Foreign Influence: What's at Stake?" *Council on Foreign Relations YouTube channel,* February 20, 2025, https://www.youtube.com/watch?v=vEj8csfVpN0.

99 Interview #6.

100 Interview #6.

101 Willoughby Fortunoff, Cheryl Martens, and Jenny Albarracín Méndez. "A Space for Kinship in City Diplomacy: Re-imagining Sister Cities amid Global Migration," *The Hague Journal of Diplomacy* 20, no. 1 (2025): 132-162, doi: https://doi.org/10.1163/1871191x-bja10199.

102 Larry Diamond and Orville Schell, "State and Local Governments," in *China's Influence & American Interests*, Hoover Institution Press, November 29, 2018, https://www.hoover.org/sites/default/files/research/docs/05_diamond-schell_sec02_web.pdf.

103 Interview #2

104 "Blackburn, Hawley: Sister city partnerships may be China's newest political weapon," Office of Senator Marsha Blackburn, October 8, 2020, https://www.blackburn.senate.gov/index.php/2020/10/blackburn-hawley-sister-city-partnerships-may-be-china-s-newest-political-weapon.

105 *Homeland Threat Assessment 2025*, U.S. Department of Homeland Security.

106 Interview #5.

107 Larry Diamond and Orville Schell, "State and Local Governments."

108 Interview #2.

109 Michael Pompeo, "U.S. States and the China Competition," U.S. Department of State, https://2017-2021.state.gov/u-s-states-and-the-china-competition/index.html.

110 "Safeguarding Our Future: Protecting Government and Business Leaders at the U.S. State and Local Level from People's Republic of China (PRC) Influence Operations," National Counterintelligence and Security Center, Office of the Director of National Intelligence, July 6, 2022, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/PRC_Subnational_Influence-06-July-2022.pdf.

111 Interview #5

112 Interview #2

113 Interview #2

114 "Stefanik, Moolenaar Introduce Washington Sister Cities Act to Terminate D.C.–Beijing Partnership and Combat CCP Influence," *Office of Congresswoman Elise Stefanik,* July 17, 2025, https://stefanik.house.gov/2025/7/stefanik-moolenaar-introduce-washington-sister-cities-act-to-terminate-dc-beijing-partnership-and-combat-ccp-influence.

115 Leslie Bonilla Muñiz, "Banks calls on Carmel to withdraw from Chinese sister city agreement," *Indiana Capital Chronicle*, January 30, 2024, https://indianacapitalchronicle.com/briefs/banks-calls-on-carmel-to-withdraw-from-chinese-sister-city-agreement/.

116 Kyle A. Jaros and Sara A. Newland, *Bridges or Battlegrounds? American Cities in a Changing US-China Relationship*.

117 "California, Shanghai Leadership Collaborate to Advance Green Shipping Corridor," California Air Resources Board, March 18, 2025, https://ww2.arb.ca.gov/news/california-shanghai-leadership-collaborate-advance-green-shipping-corridor

118 Geoff Brown and Colin Ahern, "NYC Cyber Command on Cyber Resilience. " *Global Cyber Alliance YouTube channel*, October 12, 2020, https://www.youtube.com/watch?v=wBOX13S3mVc&t=34s.

119 "Governor Hochul Signs Landmark Legislation to Strengthen Cybersecurity Across New York's Municipalities," Office of Governor Kathy Hochul, June 27, 2025, https://www.governor.ny.gov/news/governor-hochul-signs-landmark-legislation-strengthen-cybersecurity-across-new-yorks.

120 "Executive Order 50," Office of the Mayor of the City of New York, https://www.nyc.gov/office-of-the-mayor/news/50-002/executive-order-50.

121 *The Council of the City of New York v. Adams,* Index No. 154909/2025 (N.Y. Sup. Ct., N.Y. County, September 8, 2025), Final Decision and Order on Motion, https://council.nyc.gov/press/wp-content/uploads/sites/56/2025/09/ICE-on-Rikers-Final-Order-and-Judgment-1.pdf.

122 Bianca Pallaro, Jay Root, Michael Forsythe, and William K. Rashbaum, "Adams Faces Questions Over China-Linked Campaign Donor," *New York Times*, March 18, 2025, https://www.nytimes.com/2025/03/18/nyregion/adams-china-campaign-corruption.html.

123 "New York City Resident Pleads Guilty to Operating Secret Police Station of the Chinese Government in Lower Manhattan," *U.S. Attorney's Office for the Eastern District of New York*, December 18, 2024, https://www.justice.gov/usao-edny/pr/new-york-city-resident-pleads-guilty-operating-secret-police-station-chinese.

124 "Man Pleads Guilty to Conspiring to Act as Illegal Agent of the Chinese Government in the United States," U.S. Department of Justice, September 16, 2025, https://www.justice.gov/opa/pr/man-pleads-guilty-conspiring-act-illegal-agent-chinese-government-united-states.

125 "Cyber and Financial Crimes Division," Houston Police Department, https://www.houstontx.gov/police/divisions/cyber_&_financial_crimes/index.htm.

126 "Houston Police Department Annual Report 2019," Houston Police Department, 2019, https://www.houstontx.gov/police/department_reports/2019_HPD_Annual_Report_Web.pdf.

127 Alamdar Hamdani and Lucy Porter, "Cybersecurity and the Role of State and Local Governments," *The Houston Lawyer,* March/ April 2025, https://www.bracewell.com/wp-content/uploads/2025/04/Cybersecurity-Article_Hamdani-Porter.pdf.

128 Alamdar Hamdani and Lucy Porter, "Cybersecurity and the Role of State and Local Governments."

129 "Cyber Security Training," Texas Municipal League Intergovernmental Risk Pool, https://info.tmlirp.org/cyber-security-training.

130 "Cybersecurity Clearinghouse," Texas Municipal League, https://www.tml.org/199/Cybersecurity-Clearinghouse.

131 "High Intensity Drug Trafficking Areas Program Annual Report to Congress," Office of National Drug Control Policy, 2024, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/2024-HIDTA-Annual-Report-to-Congress.pdf.

132 "Houston Regional Intelligence Service Center Privacy Policy," Houston Police Department, 2009, https://www.brennancenter.org/sites/default/files/analysis/Hous.%20Fusion%20Center%20-%20Privacy%20Policy.pdf.

133 "U.S. Orders China to Close Houston Consulate," *The New York Times*, July 22, 2020, https://www.nytimes.com/2020/07/22/world/asia/us-china-houston-consulate.html; "Briefing With Senior U.S. Government Officials on the Closure of the Chinese Consulate in Houston, Texas," U.S. Department of State, https://2017-2021.state.gov/briefing-with-senior-u-s-government-officials-on-the-closure-of-the-chinese-consulate-in-houston-texas/.

134 Jay Jordan, Nicole Hensley, Samantha Keterrer, and Julian Gill, "Fire at Chinese Consulate in Houston as U.S. Orders Closure," *Houston Chronicle*, July 21, 2020, https://www.houstonchronicle.com/news/houston-texas/houston/article/fire-consulate-china-houston-texas-us-close-police-15424795.php.

135 Nicole Hensley, "Fire out at Houston consulate, but tensions flare," *CT Post*, July 22, 2020, https://www.ctpost.com/news/houston-texas/houston/article/Fire-out-at-Houston-consulate-but-tensions-flare-15427482.php.

136 "Iowa cybersecurity is national security," *Des Moines Register*, July 19, 2022, https://eu.desmoinesregister.com/story/opinion/columnists/2022/07/19/iowa-cybersecurity-national-security-fbi/10100594002/.

137 "State Cybersecurity Conference," Center for Cybersecurity Innovation & Outreach at Iowa State University, October 16, 2025, https://www.cyio.iastate.edu/state-cybersecurity-conference.

138 "New CARD Report Examines Possible Reciprocal Tariff Impacts on Iowa's Economy," Center for Agricultural and Rural Development, Iowa State University, July 24, 2025, https://www.card.iastate.edu/news/2025/new-card-report-examines-possible-reciprocal-tariff-impacts-iowas-economy.

139 Jeff Jutton and Kriss Nelson, "Building Relationships Across the Pacific," Iowa Soybean Association, January 11, 2024, https://www.iasoybeans.com/newsroom/article/isr-january-2024-building-relationships-across-the-pacific.

140 Jeff Jutton and Kriss Nelson, "Building Relationships Across the Pacific."

141 "Chairman Moolenaar Urges Local Leaders to End Ties With Chinese Communist Party Front Groups," U.S. House Select Committee on the Chinese Communist Party, August 18, 2025, https://selectcommitteeontheccp.house.gov/media/press-releases/chairman-moolenaar-urges-local-leaders-to-end-ties-with-chinese-communist-party-front-groups.

142 Caleb Geer, "U.S. House Committee Urges Des Moines to Cease Student Exchanges With China," *We Are Iowa,* August 20, 2025, https://www.weareiowa.com/article/news/local/us-house-committee-urges-des-moines-cease-student-exchanges-china/524-5e9af462-4930-4966-ba94-126934d74c72.

143 "DEA arrests 29 Iowans linked to Mexican drug cartels," *Des Moines Register*, May 18, 2023, https://www.desmoinesregister.com/story/news/crime-and-courts/2023/05/18/dea-arrests-29-iowans-linked-to-mexican-drug-cartels-sinaloa-jalisco/70207866007/.

144 Garret Leahy, "San Francisco battles rising cybercrime tsunami after Oakland hit hard," *San Francisco Standard*, March 16, 2023, https://sfstandard.com/2023/03/16/san-francisco-battles-rising-cybercrime-tsunami-after-oakland-hit-hard/.

145 Kevin Collier, "Hackers leak sensitive files after attack on San Francisco transit police," *NBC News*, January 10, 2023, https://www.nbcnews.com/tech/security/hackers-leak-sensitive-files-attack-san-francisco-transit-police-rcna65071.

146 Julie Pattinson-Gordon, "Cross-agency planning key to cybersecurity in San Francisco," *Government Technology*, January/February 2024, https://www.govtech.com/workforce/cross-agency-planning-key-to-cybersecurity-in-san-francisco.

147 Julie Pattinson-Gordon, "Cross-agency planning key to cybersecurity in San Francisco."

148 Kyle A. Jaros and Sara A. Newland, *Bridges or Battlegrounds? American Cities in a Changing US-China Relationship*.

149 Fan Dai, Jerry Brown, Zhenhua Xie, Yi Wang & Peng Gong, "How provinces and cities can sustain US–China climate cooperation," *Nature*, December 2, 2024, https://www.nature.com/articles/d41586-024-03919-9.

150 Kyle A. Jaros and Sara A. Newland, *Bridges or Battlegrounds? American Cities in a Changing US-China Relationship*.

151 Mara HvistendahlHeather Knight and Vik Jolly, "China courts U.S. cities with pandas, partnerships and access," *The New York Times*, December 19, 2024, https://www.nytimes.com/2024/12/19/world/asia/china-influence-city-local-government-pandas-intelligence.html.

152 Kyle A. Jaros and Sara A. Newland, *Bridges or Battlegrounds? American Cities in a Changing US-China Relationship*.

153 "2023 Adopted Resolutions - Support Urgent and Increased Federal Enforcement and Public Health Interventions to Address the Fentanyl Crisis," United States Conference of Mayors, 2023, https://legacy.usmayors.org/resolutions/91st_Conference/proposed-review-list-full-print-committee-individual.asp?resid=a0F4N00000S4v5pUAB.

154 "Trump orders federal agents to San Francisco amid immigration dispute," *USA Today*, October 23, 2025, https://www.usatoday.com/story/news/nation/2025/10/23/donald-trump-federal-agents-san-francisco-immigration/86844674007/.

155 Kent German and Gillian Mohney, "What we know about National Guard, other federal agents coming to San Francisco," *SFGate*, October 23, 2025, https://www.sfgate.com/bayarea/article/sf-national-guard-timeline-21114789.php.

156 "Engaging with the PRC," *ALLIES: Alliance for Local Leaders International*, 2025, https://cdn.prod.website-files.com/68bf59aba019578ada839bf7/68c48ca72744d622270766e2_ALLIES%20PRC%20Guidance%203.0.pdf.

157 Kyle A. Jaros and Sara A. Newland, *Bridges or Battlegrounds? American Cities in a Changing US-China Relationship*.

158 Lorenzo Kihlgren Grandi and Cecilia Emma Sottilotta, *When City Diplomacy Meets Geopolitics: A Framework to Help Cities Navigate Geopolitical Risk*.

Appendix 1: Interview Table

#	Interview Date	Expert Affiliation
1	April 2025	White House, Cybersecurity (former)
2	March 2025	U.S. Department of State, Subnational Diplomacy Unit (former)
3	March 2025	Centre for Public Impact
4	February 2025	University of Melbourne
5	February 2025	University of Notre Dame
6	February 2025	Smith College
7	March 2025	U.S. Department of Defense, Office of Intergovernmental Affairs (former)
8	April 2025	U.S. Department of State, Western Hemisphere Affairs; U.S. Department of Defense, Homeland Defense and Hemispheric Affairs (former)
9	April 2025	Universidad Iberoamericana Ciudad de México
10	April 2025	Atlantic Council
11	May 2025	U.S. Department of Customs and Border Protection, Office of Intergovernmental Affairs
12	May 2025	Carnegie California; U.S. Department of State (former)
13	September 2025	U.S. Defense Intelligence Agency
14	November 2025	Geopolitical risk advisory firm; U.S. intelligence community (former)
15	November 2025	Alliance for Global Security
16	November 2025	National Fusion Center Association

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org

HARVARD Kennedy School
BELFER CENTER

50 YEARS
OF RESEARCH, POLICY, AND LEADERSHIP

Printed in the United States of America