Aspen Institute Germany

Laboratories of Democracy Initiative

Critical Infrastructure

Policy Recommendations

Content

About the Project

The Laboratories of Democracy initiative brings together a total of 30 representatives from U.S. state legislatures, German *Landtage,* and Canadian provincial legislatures to facilitate a values-based discussion and exchange of ideas on how to address current international policy challenges at the subnational level.

U.S. Supreme Court Justice Louis Brandeis once wrote about the power of states as the "laboratory of democracy," where new and innovative policy approaches can be tested.

This project draws on that notion, focusing on the role of state legislators in creating policy solutions and fostering transatlantic relations in times when national governments are dominated by political polarization and crisis management. At the same time, the program encourages peer-learning and helps to build networks beyond the capitals.

In 2024, the exchange focused on the topic of critical infrastructure and the threats these systems face from cyber and physical attacks, but also natural disasters and health crises. To address these issues, the project provides a platform for exchanging innovative ideas and best practices that are necessary to develop long-term strategies and sustainable growth trajectories to positively shape policy-making and mitigate negative effects.

The participating delegates came from a large number of German *Länder*, U.S. states, and Canadian provinces. The bipartisan composition of the group underscored the participants' desire to jointly work on solutions and to strengthen transatlantic relations.

This one-year-long exchange consisted of multiple digital meetings and two in-person meetings in Mainz, Rhineland-Palatine, Germany and Austin, Texas, United States. The participants had the opportunity to engage with each other and to meet with representatives from academia, the public and private sector, and government. Based on this process, the participants developed the following bipartisan policy recommendations.

The project is supported by the Transatlantic Program of the Federal Republic of Germany, funded by the European Recovery Program (ERP) of the Federal Ministry for Economic Affairs and Climate Action (BMWK).

Preamble

Critical infrastructure is the backbone of modern and well-functioning societies, including Germany, the United States, and Canada. Unfortunately, critical infrastructures are increasingly under threat on both sides of the Atlantic from natural disasters, health crises, as well as physical and cyberattacks.

Critical infrastructure refers to those systems, organizations, facilities, assets, services, and networks that are essential to the well-functioning (safety, health, security, rule of law, and justice) of societies. Critical infrastructure can be physical or virtual, public or private.

Due to interdependencies, the disruption, corruption, or dysfunction of critical infrastructure in one sector often has dramatic consequences for the whole society. Critical infrastructures are, among others: energy; water; transportation; food and agriculture; information technology, telecommunication and media; state administration; healthcare; waste and recycling; finance and insurance; cultural heritage. In this context, the secure management and distribution of critical infrastructure constitute critical functions and a responsibility of both governments and the private sector.

In so doing, public authorities should pay special attention to those segments of the population who have tended to be underresourced and underserved both socio-economically and/or geographically. In all three countries, underserved communities and citizens have often historically had less access to critical infrastructure and their needs have not always been sufficiently considered in policies which aim to improve infrastructure resilience.[1] This affects all three risk clusters identified in this publication.

Public authorities, in cooperation with other infrastructure stakeholders, should aim to provide access and give a voice to all relevant stakeholders, regardless of race, color, creed, sex, sexual orientation, gender identity, age, disability, ancestry, national origin[2] or geographic location. This is particularly important in the development, updating, and rebuilding of critical infrastructure with the goal to foster societies in which all people are treated fairly and justly.

Subnational governments play a fundamental role in proactively safeguarding the security and functionality of critical infrastructure, but also in developing guidelines for responding to potential disruptions. As a result, they are often at the forefront of such disasters, as they are closer to affected communities and play a key role in emergency response operations. They also play a key role in coordinating with other levels of government and non-governmental organizations to ensure a coordinated and effective response.

The state and provincial legislators from Germany, the United States, and Canada who participated in the Laboratories of Democracy Initiative 2024 have proposed the following recommendations for the three threat clusters: natural disasters, health crises, as well as cyber and physical attacks. All three risk clusters carry equal importance. While these subtopics are interconnected, they each present unique challenges, which need to be explored and examined separately. These recommendations should be adapted based on local cultural and political sensibilities. The document should also be interpreted as a “living document”, with the understanding that terminologies and concepts evolve and progress.

Overall, there is a political responsibility to learn from the lessons of past critical infrastructure crises and failures and adopt appropriate policy measures. Subnational governments should establish a permanent committee to regularly and systematically review the resilience and vulnerability of critical infrastructures, past responses to emergencies, and anticipate future incidents.

Ultimately, the accordant recommendations presented here are guided by the goal of supporting and protecting fair, economically viable, environmentally sustainable, and future-oriented critical infrastructures.

© Landtag Rheinland-Pfalz

[1] See for example: Ifo Institute Munich, Strukturwandel in ländlichen Räumen, April 2024, https://www.ifo.de/DocDL/ifo_Forschungsbericht_141_Strukturwandel-laendliche-Raeume.pdf (accessed June 18, 2024); Public Health Agency of Canada, Key Health Inequalities in Canada A National Portrait, August 2018, https://www.canada.ca/content/dam/phac-aspc/documents/services/publications/science-research/key-health-inequalities-canada-national-portrait-executive-summary/hir-executive-summary-eng.pdf (accessed June 18, 2024); Ian O. Davies, “The unequal vulnerability of communities of color to wildfire, PloS One, November 2018, Volume 13, Number 11, https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0205825 (accessed June 18, 2024).

[2] The language in this sentence reflects the Equality of Rights Amendment, Nevada Constitution, Article 1., Section 24, https://www.leg.state.nv.us/const/nvconst.html (accessed June 20, 2024).

Natural Disasters

Critical infrastructure is highly vulnerable to disruption and destruction from natural disasters. Such "violent, sudden and destructive change[s] in the environment"[3] encompass a wide range of phenomena, including storms, extreme precipitation, heat waves, droughts, (forest) fires, and earthquakes. In addition, (forest) fires, earthquakes, and rising sea levels pose a significant threat to critical infrastructure.[4] According to empirical data[5], the number of floods and other hydrological events worldwide has quadrupled since 1980 and doubled since 2004. Simultaneously, extreme temperatures, storms, droughts, and forest fires have doubled since 1980. Measures should be taken to address these new realities.

Infrastructure damage from natural disasters often leads to widespread disruptions in essential services, hindering emergency response efforts and exacerbating the overall impact on affected communities. Loss of electricity, water supply, and transportation routes can impede the delivery of medical aid, food, and clean water. Additionally, the financial burden of repairing and reinforcing infrastructure post-disaster can strain government budgets and delay recovery efforts, prolonging the period of vulnerability for affected regions.

Germany, the United States, and Canada have all experienced recent cases of natural disasters affecting their critical infrastructures. In 2021, a flood devastated the Benelux countries and Germany, claiming at least 230 lives[6] and causing widespread damage to infrastructure, including drinking water and communication systems, and prolonged disruptions to gas and electricity supplies. Total damage amounted to at least 32 billion EUR (34.9 billion USD)[7].[8]

In the United States, a severe winter storm in February 2021 led to extensive power outages, primarily in Texas, affecting over five million households and resulting in more than 240 fatalities,[9] with an estimated cost of 26.8 billion USD (24.7 billion EUR)[10], making it the most expensive winter storm ever recorded in the United States.[11]

[3] European Environment Agency, EEA Glossary, https://www.eea.europa.eu/help/glossary/eea-glossary/natural-disaster (accessed April 22, 2024).

[4] Vasko Popovski, Critical Infrastructure must be Resilient…it's Critical, United Nations Development Programme, https://www.undp.org/eurasia/blog/critical-infrastructure-must-be-resilientits-critical (accessed April 25, 2024).

[5] See for example: European Academies' Science Advisory Council, Extreme Weather Events in Europe: Preparing for Climate Change Adaptation: An Update on EASAC's 2013 Study, https://www.ae-info.org/ae/Acad_Main/Publications/Press_release/Increased%20frequency%20of%20extreme%20weather%20events (accessed May 13, 2024); Intergovernmental Panel on Climate Change, Climate Change 2021, The Physical Science Basis, https://report.ipcc.ch/ar6/wg1/IPCC_AR6_WGI_FullReport.pdf (accessed July 3, 2024).

[6] Meagan Fitzgerald et al., "Almost 200 Dead, Many still Missing after Floods as Germany Counts Devastating Cost," in: NBC News, July 19, 2021, https://www.nbcnews.com/news/world/almost-200-dead-many-still-missing-after-floods-germany-counts-n1274330 (accessed April 22, 2024).

[7] Euro to US-Dollar exchange rate 1.09 (accessed July 16, 2024).

[8] Susanna Mohr et al., "A Multi-Disciplinary Analysis of the Exceptional Flood Event of July 2021 in Central Europe – Part 1: Event Description and Anaylsis," in: Natural Hazards and Earth System Sciences, Art 23, no. 2, February 2023, 525-551 (accessed April 25, 2024).

[9] Brian K. Sullivan and Naureen S. Malik, "5 Million Americans Have Lost Power From Texas to North Dakota After Devastating Winter Storm", in: Time, February 15, 2021, https://time.com/5939633/texas-power-outage-blackouts/ (accessed April 22, 204).

[10] US-Dollar to Euro exchange rate 0.92 (accessed July 16, 2024).

[11] OAA National Centers for Environmental Information (NCEI), U.S. Billion-Dollar Weather and Climate Disasters, https://www.ncei.noaa.gov/

In Canada, the 2023 wildfire season was devastating, with over 6,000 fires burning an estimated 18.4 million hectares.[12] Critical infrastructure was severely impacted, leading to road closures, telecommunication disruptions, and threats to high voltage power lines. The economic costs of combatting fires in Canada are approaching 750 million CAD (549.3 million USD / 503.2 million EUR)[13] per year.[14]

[12] Europea NASA Earth Observatory, Tracking Canada's Extreme 2023 Fire Season, https://earthobservatory.nasa.gov/images/151985/tracking-canadas-extreme-2023-fire-season#:~:text=Many%of%Canada's%20fires%20in.the%20La%20Grande%20Reservoir%203 (accessed April 22, 2024).

[13] Associated Canadian Dollar to US-Dollar Exchange Rate 0.73, Canadia Dollar to Euro Exchange Rate 0.67 (accessed July 16, 2024).

[14] The Associated Press, "Wildfires in Canada have Broken Records for Area Burned, Evacuations and Cost, Official says," in: ABC News, https://web.archive.org/web/20230708014416/https://abcnews.go.com/International/wireStory/wildfires-canada-broken-records-area-burned-evacuations-cost-100806230 (accessed April 22, 2024).

© Aspen Germany

Natural Disasters

Subnational Policy Recommendations

1. Public authorities should establish and improve a state/province-wide framework for rapid response and functional recovery by ensuring an emergency-resistant power supply, redundant internet and other communications networks, food, shelter, and other supplies between states, provinces, and regions.

Action Points:

▶ Public authorities should establish processes to conduct regular and frequent tabletop exercises* coordinated by a consistent emergency management organization, considering local conditions and including different case scenarios.

▶ Where not yet existing, public authorities should establish a permanent command center at the state/provincial level, and where possible district or municipal level, and establish a process for setting up agile and mobile command centers at the local level to oversee and coordinate information and communications to rapidly respond to incidents and ensure consistent, timely and correct communications with the public and service providers.

2. Public authorities need to plan and coordinate better among agencies, stakeholders, first/tribal nations, and local governments, to establish early warning systems in order to prevent and mitigate future disasters and encourage development of resilient landscape plans.

Action Points:

▶ Public authorities should establish plans with clear lines of accountability and responsibility for immediate emergency management as well as long term recovery.

▶ Public authorities should test and practice multi-lingual communication and early warning mechanisms, with public participation, including school activities, as well as regularly update accurate and accessible signage, websites, and social media.

3. Public authorities, together with other relevant stakeholders, should ensure that rebuilding is focused on improving the resilience of infrastructure, taking into consideration the needs and vulnerabilities of affected communities, groups, and individuals.

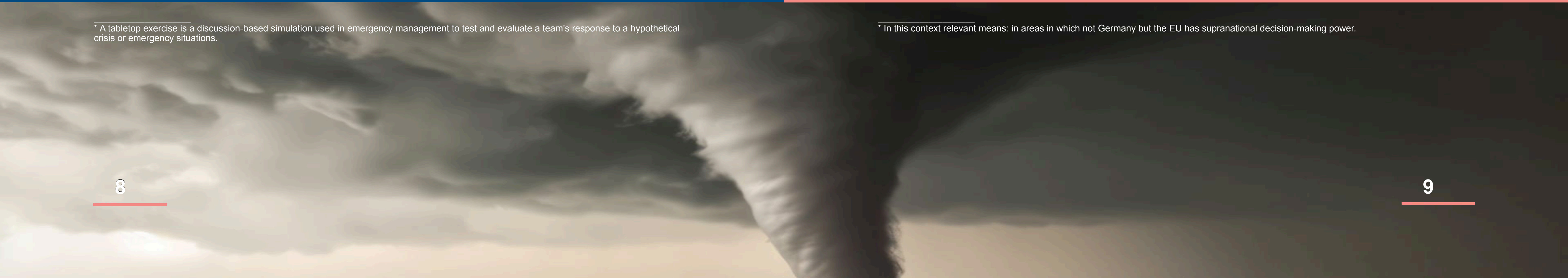
Action Points:

▶ Public authorities, with input from other relevant stakeholders, should identify risk areas with disaggregated data and define regulations for (re)construction to protect against natural disaster, strengthen resilience, and explore possible disaster recovery assistance policies.

▶ Public authorities, together with other relevant stakeholders, should regularly assess critical infrastructure based on historical data and forecasts to identify vulnerabilities in existing infrastructure as well as future infrastructure needs and integrate the findings in infrastructure planning.

Transatlantic Policy Recommendation

The U.S., Canadian and German governments (and where relevant* the EU) should regularly update natural hazard risk analysis and forecasting, based on critical infrastructure data from the past ten years, and exchange learning across the Atlantic on their processes and data in order to enable more resilient planning for building/rebuilding critical infrastructure, hazard mitigation, and recovery planning to reduce impacts from future events.



* A tabletop exercise is a discussion-based simulation used in emergency management to test and evaluate a team's response to a hypothetical crisis or emergency situations.

* In this context relevant means: in areas in which not Germany but the EU has supranational decision-making power.

Cyber and Physical Attacks

Critical infrastructure is an important bedrock of national security, economic stability, and societal well-being, yet it faces a growing number of threats due to a myriad of factors including the interconnected nature of the modern world and of systems we depend on, as well as the growing mistrust of government, media, and established institutions. According to the Freedom House Index 2024, global security and democracy are increasingly threatened by armed conflicts and authoritarian aggression.[15]

Geopolitical conflicts, geo-economic confrontations, and the revival of great power competition have incited both physical attacks and cyberattacks on critical infrastructure. The United Nations (UN) Office of Counter-Terrorism, the UN Security Council, and Interpol have jointly emphasized the importance of national strategies for Critical Infrastructure Protection (ICP) against terrorist attacks.[16]

Attacks on critical infrastructure are deliberate acts aimed at damaging or disrupting essential services ranging from energy and transportation to communications and healthcare. The perpetrators can be organized crime syndicates with financial motivations as well as state-sponsored agents or terrorist groups pursuing political objectives.

Physical attacks often target facilities like electrical substations, oil refineries, and water treatment plants. The impact of these attacks is profound, leading to widespread service disruptions, with the potential to compromise national security, stability, and economic prosperity. The adversary employs either force, deception, or stealth to disable or bypass access controls. The attack is executed by manipulating the system functions or by directly damaging its physical components.[17]

While physical attacks are a serious threat, critical infrastructure today is predominantly targeted through cyberattacks. These attacks involve malicious activity aimed at accessing or damaging the networks and systems behind critical infrastructure to disrupt services through malware or denial-of-service attacks, steal sensitive information through fishing campaigns, extort money with ransomware attacks, or threaten democratic institutions. The digitization of critical infrastructure presents new vulnerabilities, while the increased sophistication of attacks through new technologies like AI and quantum computing maximizes their effectiveness.

In 2023, critical infrastructure emerged as the primary target for politically motivated cyberattacks, with the healthcare and financial sectors facing the highest number of attacks.[18] While 35 percent of attacks cannot be traced, of those that can be, state and non-state actors are responsible for a significant share, with nearly 13 percent originating from Russia and 6 percent from China in 2023.[19] In this context, disinformation – anticipated by the World Economic Forum's Global Risks Report 2024[20] to be the most severe global risk over the next two years – can act as a threat multiplier by undermining public trust and complicating the responses to real-time emergencies. By spreading false information about infrastructure conditions or security incidents, disinformation can cause panic and mislead public perception. Underscoring their disruptive impact, cyberattacks are estimated to account for an annual cost of 9.2 trillion USD (8.4 trillion EUR)[21] in 2024.[22]

[15] Freedom House, Freedom in the World 2024, February 2024, https://freedomhouse.org/sites/default/files/2024-02/FIW_2024_DigitalBooklet.pdf (accessed April 22, 2024).

[16] United Nations Office of Counter-Terrorism, The Protection of Critical Infrastructure Against Terrorist Attacks Compendium of Good Practices 2022 Update, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2225521_compendium_of_good_practice_web.pdf (accessed May 13,2024).

[17] G. Wyss et al., Identifying and Defeating Blended Cyber-Physical Security Threats, Sandia National Laboratories, January 1, 2007, https://www.osti.gov/servlets/purl/1427000 (accessed April 22, 2024).

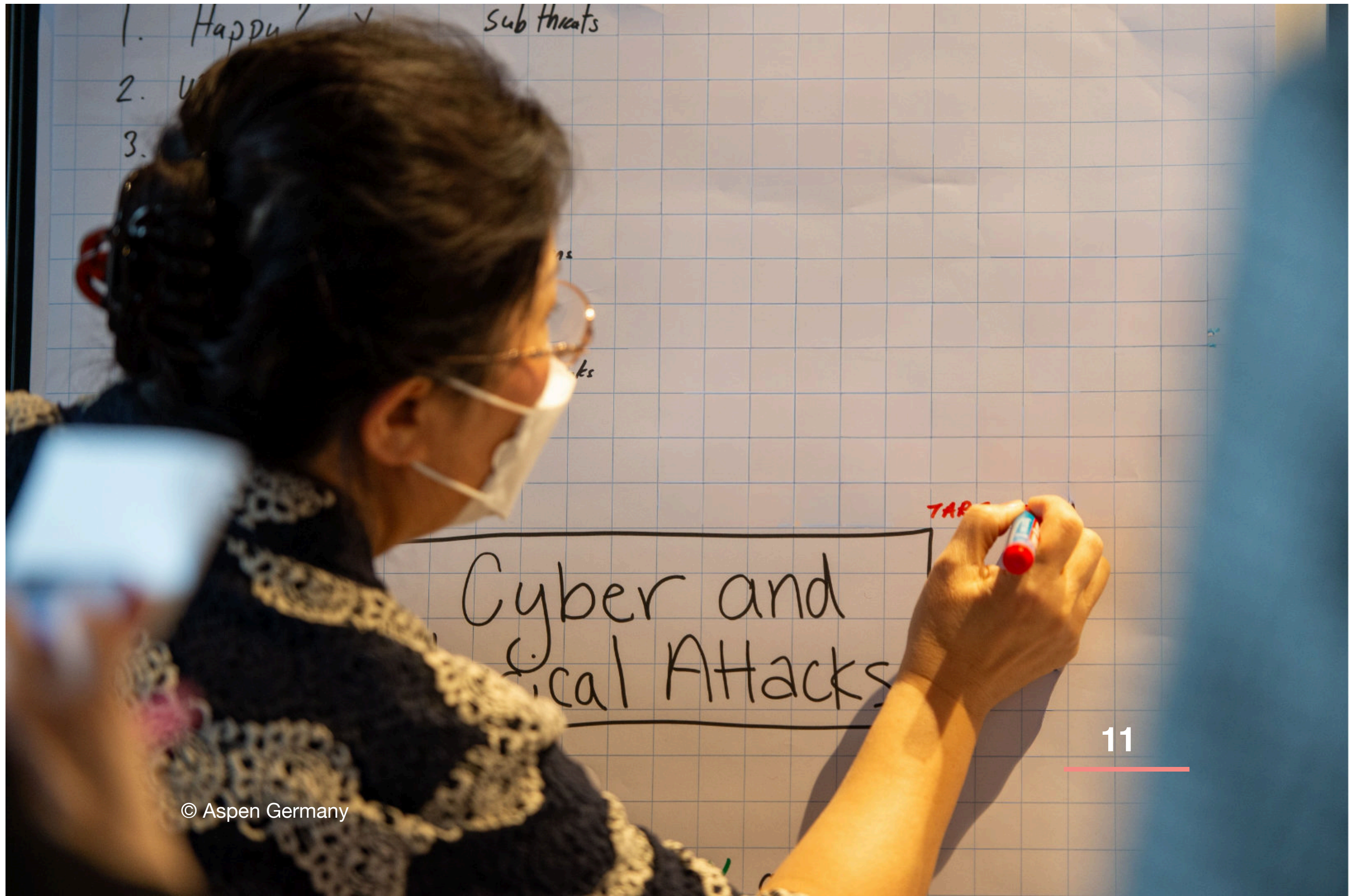
[18] Florian Zandt, The Sectors Most Targeted by Cybercrime, Statista, https://www.statista.com/chart/31985/number-of-cyber-attacks-recorded-per-sector/ (accessed April 22, 2024).

[19] Bund et al., 2023 Cyber Activity Balance, European Repository of Cyber Incidents, January 31, 2024, https://eurepoc.eu/wp-content/uploads/2024/02/Cyberkonflikt_Briefing_2023.pdf (accessed April 22, 2024).

[20] World Economic Forum, Global Risks Report 2024, January 10, 2024, https://www.weforum.org/publications/global-risks-report-2024/ (accessed April 22, 2024).

[21] US-Dollar to Euro Exchange Rate 0.92 (accessed July 16, 2024).

[22] Anna Fleck, Cybercrime Expected to Skyrocket in Coming Years, Statista, https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/, (accessed April 30, 2024).



© Aspen Germany

Cyber and Physical Attacks

Subnational Policy Recommendations

1. Public authorities* should develop and regularly update minimum standards for cybersecurity.

Action Points:

▶ Because technology is rapidly changing, public authorities should regularly convene experts and critical infrastructure stakeholders to recommend minimum standards and best practices for cybersecurity in areas of critical infrastructure.

▶ Public authorities, together with experts and industries, should establish processes to implement minimum standards as well as regularly review and update current systems security.

2. Critical infrastructure stakeholders should implement secure and offline backup protocols and update backup plans to ensure redundancies in essential infrastructure systems.

Action Points:

▶ Critical infrastructure systems stakeholders should develop, test, and update immediate response plans to secure redundancies in essential infrastructure systems.

▶ Public authorities, together with critical infrastructure stakeholders, should regularly convene experts from potentially affected sectors to develop future-looking protocols for countering cyberattacks and preventing or mitigating negative impacts on critical infrastructure.

3. Public authorities and other relevant stakeholders should provide the necessary education for all levels and sectors of the society on data security and ensure the development and implementation of systems which reduce the vulnerability of infrastructures due to human error.

Action Points:

▶ Public authorities and other relevant stakeholders should support the development, implementation, and ongoing review of systems and processes to defend against cyberattacks and prevent negative impacts on critical infrastructure.

▶ Public authorities and other relevant stakeholders should take rapidly changing risk vectors into account to reduce the impact of user mistakes on system security and regularly train end users to reduce risks further.

Transatlantic Policy Recommendation

The U.S., Canadian and German governments (and where relevant the EU) should establish a common process for the timely exchange of information regarding potential weaknesses in critical infrastructure to cyber and physical attacks and for promptly addressing these vulnerabilities.

* The term “public authorities” represents national, subnational governments and elected officials in this publication.

Health Crises

Health crises such as pandemics, epidemics, endemics, and antibiotic resistance pose a significant threat not only to the healthcare sector, but also to critical infrastructure in general, particularly in an increasingly interconnected world.

The World Health Organization (WHO) defines a public health emergency of international concern as "an extraordinary event which is determined to constitute a public health risk to other states through the international spread of disease and to potentially require a coordinated international response."[23] In addition, natural disasters and deliberate attacks of all kinds (both physical and cybernetic) entail strains on health and on care services, which can lead to health crises as part of comprehensive emergency situations.

The healthcare sector, as a vital component of critical infrastructure, is inherently susceptible to these crises due to its central role in public health. However, other essential services are also at risk. For instance, transportation networks can face disruptions from travel restrictions, leading to shortages of goods and equipment. Moreover, the interconnectedness of critical infrastructure sectors means that disruptions in one sector can cascade and affect others. For example, a healthcare crisis resulting in widespread illness or workforce shortages may impact sectors reliant on healthy and available personnel, such as transportation or emergency services. Moreover, the long-term impacts of health crises may lead to disinvestment or reduced funding for critical infrastructure projects due to economic downturns. This, in turn, increases vulnerability to future disruptions and compromises the ability of critical infrastructure to withstand and recover from adverse events.

The COVID-19 pandemic is a recent and stark example of the vulnerability of our interconnected world to global health crises, where local outbreaks can swiftly cross borders through international travel and disrupt economies by halting production along supply chains. Hospitals and medical facilities faced overwhelming surges in cases, leading to critical shortages of medical supplies, equipment, and personnel. According to data by the American Hospital Association job openings for different types of nursing staff surged by as much as 30 percent from 2019 to 2020.[24] Shortage of personnel was a particularly critical bottleneck to the upgrading of intensive care units so that additional equipment could not always be put to full use.

According to WHO projections at the beginning of the COVID-19 pandemic, approximately 89 million medical masks, 76 million examination gloves, and 1.6 million goggles were going to be needed monthly for the COVID-19 response.[25]

[23] WHO, Emergencies: International Health Regulations and Emergency Committees, https://www.who.int/news-room/questions-and-answers/item/emergencies-international-health-regulations-and-emergency-committees (accessed 29 April, 2024).

[24] American Hospital Association, Data Brief, Health Care Workforce Challenges Threaten Hospitals' Ability to Care for Patients, October, 2021, https://www.aha.org/system/files/media/file/2021/11/data-brief-health-care-workforce-challenges-threaten-hospitals-ability-to-care-for-patients.pdf (accessed April 29, 2024).

[25] WHO, Shortage of Personal Protective Equipment Endangering Health Workers Worldwide, March 3, 2020, https://www.who.int/news/item/03-03-2020-shortage-of-personal-protective-equipment-endangering-health-workers-worldwide (accessed April 29, 2024).

Additionally, the prolonged duration of the pandemic brought about unique and protracted economic impacts, distinguishing it from other threats to critical infrastructures. In total, the International Monetary Fund (IMF) projected the COVID-19 pandemic to result in a cumulative output loss of approximately 13 trillion USD (12 trillion EUR)[26] through 2024, underscoring its severity and long-lasting impact.[27]

[26] US-Dollar to Euro Exchange Rate 0.92 (accessed July 16, 2024).

[27] IMF, A Global Strategy to Manage the Long-Term Risks of COVID-19, April 5, 2022, https://www.imf.org/en/Publications/WP/Issues/2022/04/04/A-Global-Strategy-to-Manage-the-Long-Term-Risks-of-COVID-19-516079 (accessed April 29, 2024).

Health Crises

Subnational Policy Recommendations

1. In non-crisis times, public authorities should work to facilitate clear, transparent, and widely known chains of command and cooperation across all potentially affected sectors, including government, business, nonprofit organizations, and private institutions with special attention to those segments of the population who have tended to be underresourced and underserved.

Action Points:

▶ Public authorities should develop, update, and communicate guidelines for best practices and action plans for potential crises and encourage stakeholder engagement.

▶ Public authorities should ensure that all relevant public officials on all levels of government are included in the chain of command and regularly consulted with the goal of better communicating accurate information to constituents.

2. Public authorities should foster an environment which allows them to effectively partner with civil society to strengthen first aid and public health education (taking into account liability issues) through programs like the U.S. Community Emergency Response Team (CERT) and National Red Cross Societies, including medical and preventive operations, fire safety, search, and rescue.

Action Points:

▶ Public authorities should provide accurate, timely, ongoing, and consistent information throughout the duration of a public health crisis.

▶ Public authorities should proactively provide resources to educate the public, starting from an early age onwards, on health emergency response, such as infection control, and first aid.

3. Public authorities, in their planning and funding for healthcare facilities, services and workforce, should efficiently take into account resilience to emergency situations.

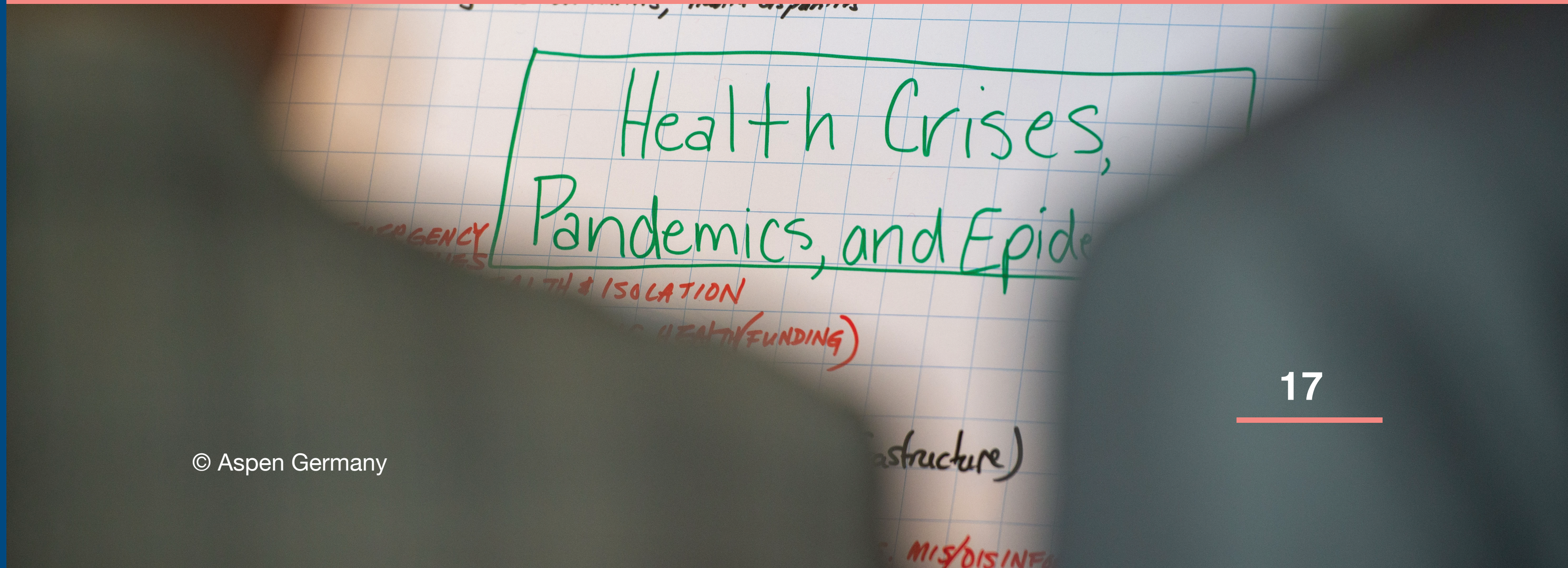
Action Points:

▶ Public authorities should establish systems for increasing or maintaining surge capacity for those entities relying on traveling nurses, doctors, and specialists to provide care, particularly in rural areas.

▶ Public authorities should improve planning for surge capacity within the healthcare system to ensure the resilience of relevant critical infrastructure during health crises.

Transatlantic Policy Recommendation

The U.S., Canadian and German governments (and where relevant the EU) should foster transatlantic cooperative surveillance of pathogens by enhancing outbreak monitoring, such as wastewater monitoring, advanced data analytics, and real-time reporting systems to enhance early detection and rapid response to infectious disease threats and support data-driven decision-making at all levels of government, recognizing that state and provincial legislatures determine policy and process for their jurisdictions.



© Aspen Germany

Authors

Representative Brad Barker (R) Member of the Montana House of Representatives

Chuck Chiasson MLA (New Brunswick Liberal Party) Critic for Transportation and Infrastructure in the Legislative Assembly of New Brunswick

Stefan Ebner MdL (CSU) Member of the State Parliament of Bavaria

Julia Eisentraut MdL (Alliance 90/The Greens) Member of the State Parliament of North Rhine-Westphalia

Alena Fink-Trauschel MdL (FDP) Member of the State Parliament of Baden-Württemberg

Lea Heidbreder MdL (Alliance 90/The Greens) Deputy Chairwoman of the Alliance 90/The Greens parliamentary group in the State Parliament of Rhineland-Palatinate

Robert Henderson MLA (Prince Edward Island Liberal Party) Opposition Whip in the Legislative Assembly of Prince Edward Island

Representative Jason Hughes (D) Member of the Louisiana House of Representatives

Bijan Kaffenberger MdL (SPD) Member of the State Parliament of Hesse

Samir Kayande MLA (New Democratic Party) Deputy Assistant Opposition Whip in the Legislative Assembly of Alberta

Cornelia Klisch MdL (SPD) Member of the State Parliament of Thuringia

Natalia Kusendova-Bashta MPP (Progressive Conservative Party of Ontario) Minister of Long-Term Care

Michael Lee MLA (BC United) Shadow Minister for Indigenous Relations and Reconciliation

Gilles LePage MLA (New Brunswick Liberal Party) Opposition Member in the Legislative Assembly of New Brunswick

Representative Karianne Lisonbee (R) Majority Whip in the Utah House of Representatives

Brandon Lunty MLA (United Conservative Party) Member of the Legislative Assembly of Alberta

Helmut Martin MdL (CDU) Deputy Chairman of the CDU parliamentary group in the State Parliament of Rhineland- Palatinate

Ansgar Mayr MdL (CDU) Member of the CDU parliamentary group executive board in the State Parliament of Baden-Württemberg

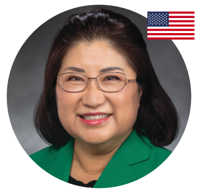
Mary-Margaret McMahon MPP (Ontario Liberal Party) Member of the Provincial Parliament of Ontario

Senator Tracy Pennycuick (R) Member of the Pennsylvania State Senate

Delegate Lily Qi (D) Member of the Maryland House of Delegates

Matthew Rae MPP (Progressive Conservative Party of Ontario) Parliamentary Assistant to the Minister of Municipal Affairs and Housing in the Legislative Assembly of Ontario

Heide Richter-Airijoki MdL (SPD) Member of the State Parliament of Saxony-Anhalt



Representative Cindy Ryu (D) Member of the Washington House of Representatives

Tanja Schorer-Dremel MdL (CSU) Deputy Chairwoman of the CSU parliamentary group in the State Parliament of Bavaria

Representative Matthew Soper (R) Member of the Colorado House of Representatives

Senator Pat Spearman (D) President Pro Tempore in the Nevada State Senate

Heather Sweet MLA (New Democratic Party) Opposition Deputy House Leader in the Legislative Assembly of Alberta

Senator Löki Gale Tobin (D) Member of the Alaska State Senate

Participants:

Representative Brad Barker, Chuck Chiasson MLA, Stefan Ebner MdL, Julia Eisentraut MdL, Alena Fink-Trauschel MdL, Representative Brian Harrison, Lea Heidbreder MdL, Robert Henderson MLA, Representative Jason Hughes, Bijan Kaffenberger MdL, Samir Kayande MLA, Cornelia Klisch MdL, Natalia Kusendova-Bashta MPP, Michael Lee MLA, Gilles LePage MLA, Representative Karianne Lisonbee, Brandon Lunty MLA, Helmut Martin MdL, Ansgar Mayr MdL, Mary-Margaret McMahon MPP, Senator Tracy Pennycuick, Delegate Lily Qi, Matthew Rae MPP, Heide Richter-Airijoki MdL, Representative Cindy Ryu, Tanja Schorer-Dremel MdL, Representative Matthew Soper, Senator Pat Spearman, Heather Sweet MLA, Senator Löki Gale Tobin.

Aspen Institute Germany

About the Aspen Institute Germany

The Aspen Institute Germany is an independent, non-partisan organization that promotes values-based leadership, constructive dialogue between conflicting parties, and transatlantic cooperation to strengthen a free and open society. Founded in 1974 in Berlin, the Institute has been bringing together decision-makers and experts from politics, business, academia, media, culture, and civil society for 50 years to address the challenges of our time.

More information about the Aspen Institute Germany:

www.aspeninstitute.de

@AspenGermany

@aspen_germany

Aspen Institute Germany

@AspenGermany

Imprint

Publisher: Aspen Institute Germany e.V.
Friedrichstraße 60, 10117 Berlin
Germany

ISSN: 2749-246X
Project Management: Dr. Stormy Mildner, Emilie Schreier, Julian Mench
Editors: Dr. Stormy Mildner, Katja Greeson, Emilie Schreier, Julian Mench, Tobias Röttger
Design & Layout: Tobias Röttger, Emilie Schreier
August 2024

Dr. Stormy Mildner
Executive Director

Katja Greeson
Program Director

Emilie Schreier
Program Officer

Julian Mench
Junior Program Officer

Tobias Röttger
Program Assistant

The project is supported by the Transatlantic Program of the Federal Republic of Germany, funded by the European Recovery Program (ERP) of the Federal Ministry of Economics and Climate Protection (BMWK).

Federal Ministry
for Economic Affairs
and Climate Action