Sandia National Laboratories

PURDUE UNIVERSITY
Institute for a Sustainable Future

CSIRO
Australia's National Science Agency

Unravelling the Cyber-Physical-Social Infrastructure Climate Change Nexus

Advanced Research Workshop
July 29–August 1, 2024
Washington, DC

This workshop is sponsored by the NATO Science for Peace and Security Programme under Grant ID G6282

U.S. DEPARTMENT OF HOMELAND SECURITY

Science & Technology

Contents

Workshop Overview

Vision: This NATO Advanced Research Workshop will formulate recommendations, conclusions, in the CPSICC Nexus and foster partnerships among experts from different nations. By the end of the workshop, we will identify R&D gaps within this nexus and set an agenda for filling these gaps.

The CPSICC Nexus Workshop represents a collaborative effort to address the critical convergence of climate change, cybersecurity, and essential infrastructure, which includes social-economic-political institutions. As our global challenges grow in complexity, understanding the intricate interplay between these domains becomes paramount in order to prepare for the future. Given the multifaceted threats posed by climate change and cyber-physical-social security, we actively seek input from experts across diverse fields. Workshop participants include academics, government officials, industry leaders, and policymakers.

Co-Directed by Matthew Huber, Director of Purdue University's Institute for a Sustainable Future and Surya Nepal, Senior Principal Research Scientist at Australia's CSIRO, this invitation-only Advanced Research Workshop is sponsored by NATO's Science for Peace and Security Program and has been co-funded by the U.S. Department of Homeland Security's Science & Technology Directorate. The workshop is convened in conjunction with Sandia National Laboratories and Purdue's Center for Education and Research in Information Assurance and Security and Policy Research Institute.

Meeting Organizers

Marthie Grobler
Principal Research Scientist
CSIRO

Surya Nepal
Senior Principal Research Scientist
CSIRO Data61

Rossitza Homan
Manager, Resilience and Regulatory Effects Department
Sandia National Laboratories

Dongyan Xu
Samuel Conte Professor of Computer Science, Director of CERIAS
Purdue University

Matthew Huber
David E. Ross Director, Institute for a Sustainable Future
Purdue University

Workshop Website
Visit the workshop website, cpsiccnexusworkshop2024.org, for read-ahead materials and more information on speakers and attendees.

Meeting Logistics

Dates
- Monday, July 29, 2–5 p.m. EDT
- Tuesday, July 30, 8 a.m.–7 p.m. EDT
- Wednesday, July 31, 8 a.m.–9 p.m. EDT
- Thursday, August 1, 8 a.m.–5 p.m. EDT

Meeting Contacts
- Karan Hustedt-Warren, khustedt@purdue.edu, 765-543-1620
- Leslie Proctor, lprocto@sandia.gov, 925-315-1596

Location – AGU Conference Center
The American Geophysical Union (AGU) Conference Center is located at 2000 Florida Ave NW, Washington DC. AGU is an association of Earth and space scientists with over 60,000 members, worldwide, extending to an even wider community of over 130,000 enthusiasts and environmental stewards, through partnerships and education, dedicated to discovery AND solution science to "accelerate knowledge and create solutions that are ethical, unbiased, and respectful of communities and their values." As testament to the AGU mission and purpose, the AGU Building reopened in 2019, after an extensive renovation, making AGU the first refurbished facility in the greater D.C. area designed for net-zero-energy consumption. The unique engineering re-design utilizes principles of reduction, reclamation, absorption and generation to target our net zero energy goals. Learn more at www.agu.org/building.

The workshop will convene on the Lobby level. Breakout rooms will be used for the gameplay sessions.

Accessibility
The AGU building, including the conference facilities, is fully ADA compliant to all current standards.

Getting There
- Public transportation: The closest Metro Station is Dupont Circle on the Red Line. We are located about 3 blocks North of the station. Car-sharing services are also readily available.
- Parking: Some metered street parking is available. Consider a parking app such as Spot Hero to identify and schedule parking in real time, based upon your destination. Nearby parking areas include Colonial Parking (1875 Connecticut Ave. NW or 1919 Massachusetts Ave. NW), LAZ Parking Garage (2001 S St. NW), and ONE Parking Garage (1666 Connecticut Ave. NW).

Internet
All participants will have access to the house Wi-Fi network:
- Name: AGU Guest WiFi
- Password: Welcome2net0%

Food Notes
A light breakfast, lunch, and afternoon tea/coffee service with snacks will be provided Tuesday, Wednesday, and Thursday. Dinner will be provided Tuesday and Wednesday. Vegetarian/vegan and gluten free options will be available.

Meeting Code of Conduct
AGU adheres to a program called "SAFE AGU" which is designed to ensure that ALL attendees of AGU meetings are welcomed and comfortable, throughout all facets of the meeting experience. Please review the meeting code of conduct at www.agu.org/plan-for-a-meeting/agumeetings/meetings-resources/meetings-code-of-conduct.

Agenda

Monday, July 29

2:00 PM	**Registration/Initial Icebreaker**
3:00 PM	**Welcome, Introductions, and Expectations:** Matthew Huber, Purdue University; Marthie Grobler, CSIRO; Rossitza Homan, Sandia National Laboratories; James Appathurai, NATO Deputy Assistant Secretary General; Julie Brewer, Deputy Under Secretary, U.S. DHS S&T
3:45 PM	**Setting the Scene:** *Laying out the landscape of the CPSICC NEXUS through 2050* — David Johnson, Purdue University
4:00 PM	**Plenary Talk:** *Emerging security challenges* *DHS strategic line of effort* — David Alexander, U.S. DHS S&T *NATO strategic line of effort* — Eyüp Turmuş, NATO SPS Programme
5:00 PM	**Adjourn**

Tuesday, July 30

8:00 AM	**Registration and Light Breakfast**
8:30 AM	**Introduction/Initial Exhortation:** Matthew Huber, Purdue University
9:00 AM	**Talk:** *Future climate change and insights into the implications for energy, communities, and economies* — Richard Matear, CSIRO
9:35 AM	**Talk:** *The first European Climate Risk Assessment: How to support policy prioritisation in a complex risk and political context* — Hans-Martin Füssel, European Environment Agency
10:10 AM	**Coffee Break**
10:30 AM	**Talk**: *Compound and cascading climate hazards and their impacts on critical infrastructure systems* — Amir AghaKouchak, University of California Irvine
11:05 AM	**Talk:** *Cybersecurity and climate change nexus: Applying risk-based approaches to ensure resilience and critical mission assurance of cyber-physical systems* — Piret Pernik, NATO Cooperative Cyber Defence Centre of Excellence
11:35 AM	**Talk**: *Extreme weather trends against datacenters and cryptocurrency functionality* — Sunny Wescott, U.S. DHS
12:00 PM	**Networking Lunch** (food will be provided)
1:00 PM	**Short Talks** *Not breaking the bank: Where climate technology could maintain financial system stability* — Nick Heavens, Viridien *The challenge of adaptation seen through the lens of complexity* — Giovanni Fusina, Defence Research and Development, Canada *Policy response to climate and the role of community representatives* — David Kaufman, CNA *National critical infrastructures: The need for addressing cascading effects and cross-sector governance* — Jonas Johansson, Lund University *Climate change, security, and misinformation* — Tom Ellison, Center for Climate and Security *Beyond the trend: The superposed impacts of climate change and variability on cyberinfrastructure* — Christina Karamperidou, University of Hawai'i at Mānoa *Stress testing in the context of supply-chain resilience and financial-sector resilience* — Mark Flood, University of Maryland *Improving global security, deterrence and defense: Cyber-physical-social systems and climate change nexus perspectives* — Rossitza Homan, Sandia National Laboratories

Agenda

Tuesday, July 30—continued

2:45 PM   **Panel Discussion with Presenters** and including Igor Linkov, U.S. Army Engineer Research and Development Center, and Lilian Alessa, University of Idaho
Facilitator: Marthie Grobler, CSIRO

3:15 PM   **Coffee Break**

3:30 PM   **Plenary Talk:** *Climate security and integrated deterrence* — Rob Leland, Sandia National Laboratories

4:00 PM   **Talk:** *Risks and opportunities for cybersecurity posed by quantum technology* — Marcin Niemiec, AGH University of Science and Technology Stanisław Staszic in Krakow

4:30 PM   **Introduction to Smart Games and CPSICC Gameplay**

5:00 PM   **Evening Mixer, Lightning Talks** (food will be provided)
Joel Rasmus, Purdue University
Stacey Connaughton, Purdue University
Ben Bonin, Sandia National Laboratories
Tim Judge, Fannie Mae
Igor Linkov, U.S. Army Engineer Research and Development Center
Anjuli Bamzai, NSF GEO
Nuna Mota, Fannie Mae

7:00 PM   **Adjourn**

Wednesday, July 31

Morning Session

8:00 AM   **Registration and Light Breakfast**

8:30 AM   **Introductory Talk:** *From threat multiplier to opportunity multiplier in climate security and infrastructure resilience* — Sherri Goodman, Wilson Center

9:00 AM   **Setup and Scenario Building**

9:30 AM   **Gameplay**
1) Near term to 2030
2) Scenario role play 1
3) Scenario role play 2

12:00 PM   **Lunch with Game Groups** (food will be provided)

Afternoon Session

1:00 PM   **Gameplay**

2:30 PM   **Coffee Break**

2:45 PM   **Summary of Game Results and Report Out**

Agenda

3:45 PM	**Short Talks**
	Modeling human dynamics for critical infrastructure resilience — Budhendra (Budhu) Bhaduri, Oak Ridge National Laboratory
	Is cybersecurity turning up the heat on climate change? — Helge Janicke, Cyber Security Cooperative Research Centre, Australia
	Human-centered cyber security — Giovanni Russello, Auckland University
	Climate risks, uncertainties, and economic opportunities — Gernot Wagner, Columbia Business School
	Three worldviews for complex systems — Thushara Gunda, Sandia National Laboratories
5:00 PM	**Break**
6:00 PM	**Banquet with TED-style Talks** (food will be provided)
	Emerging climate risks: An inconvenient truth — Malcolm Mistry, Ca' Foscari University of Venice, Italy and Environment & Health Modelling Lab, The London School of Hygiene & Tropical Medicine, UK
	Swathi Veeravalli, National Security Council
	Robert Kopp, Rutgers University
	Kellee Wicker, Wilson Center
	Lilian Alessa, University of Idaho
	Honor Sangster, UK Ministry of Defence
9:00 PM	**Adjourn**

Thursday, August 1

Morning Session

8:00 AM	**Registration and Light Breakfast**
8:30 AM	**Setup and Scenario Building**
9:00 AM	**Gameplay**
11:00 AM	**Summary Discussion**
12:00 PM	**Lunch with Game Groups** (food will be provided)

Afternoon Session

1:00 PM	**Group Work, SWOT Analysis, Next Steps, and Identifying Research Gaps**
4:00 PM	**Closing Remarks**
5:00 PM	**Adjourn**

Featured Speakers

Amir AghaKouchak
Chancellor's Professor, Department of Civil & Environmental Engineering, University of California, Irvine

Amir AghaKouchak is a Professor of Civil and Environmental Engineering and Earth System Science at the University of California, Irvine. He is the Lead for Water, Climate and Infrastructure Risk at the United Nations University Institute for Water, Environment and Health. His research focuses on natural hazards and climate extremes and crosses the boundaries between hydrology, climatology, and remote sensing. One of his main research areas is studying and understanding the interactions between different types of climatic and non-climatic hazards, including compound and cascading events. AghaKouchak has published 240 peer-reviewed research articles in scientific journals. He has received several honors and awards, including the American Geophysical Union's James B. Macelwane Medal, Fellow of AGU, and the American Society of Civil Engineers Norman Medal and Huber Research Prize.

James Appathurai
Deputy Assistant Secretary General, NATO

James Appathurai was appointed to the post of NATO's Deputy Assistant Secretary General for Innovation, Hybrid and Cyber in September 2021. As DASG, he works on policy development and implementation in the fields of Emerging and Disruptive Technologies, cyber security, energy security, the security implications of climate change, the protection of critical infrastructure, and hybrid defence. Appathurai previously served as DASG for Political Affairs and Security Policy, as well as Special Representative to Central Asia and the Caucasus. He was NATO's Spokesperson from 2004 to 2010. He served as Deputy Head and Senior Planning Officer in the Policy Planning and Speechwriting Section of NATO's Political Affairs Division from 1998 to 2004. He served in the Canadian Defence Department from 1994 to 1998.

David Alexander
Senior Science Advisor for Resilience, U.S. Department of Homeland Security S&T

David Alexander serves as the Senior Science Advisor for Resilience within the U.S. Department of Homeland Security Science & Technology Directorate. In this role, he leads innovative research on Homeland Security preparedness and disaster resilience. Alexander's work focuses on enhancing knowledge, advancing state-of-the-art, and informing investments to address national threats, hazards, and risks. He also serves as co-chair for the National Science and Technology Committee\Subcommittee on Resilience Science and Technology and as a DHS representative to the U.S. Global Change Research Program.

Julie Brewer

Deputy Under Secretary for Science and Technology, U.S. Department of Homeland Security

Julie Brewer is the Deputy Under Secretary for the U.S. Department of Homeland Security Science and Technology Directorate, which is responsible for identifying operational gaps, conceptualizing art-of-the-possible solutions, and delivering operational results that improve the security and resilience of the nation. Previously, Brewer served as the Executive Director of the Office of Innovation and Collaboration, where she provided access to technology-based capabilities and solutions through a vast network of trusted partnerships and manages tools and contract mechanisms that allow S&T to sponsor critical research and development. Brewer previously served S&T as the Senior Official Performing the Duties of the Chief of Staff for S&T and the Director of the Office of National Laboratories. Brewer began her career as an officer in the U.S. Air Force. She is a recipient of the 2022 Meritorious Presidential Rank Award and the 2021 DHS Secretary's Leadership Excellence Award.

Hans-Martin Füssel

Coordinator, European Climate Risk Assessment, European Environment Agency

Hans-Martin Füssel has more than 25 years of experience in climate change research and policy advice. Füssel works as an expert on climate risks and adaptation at the European Environment Agency in Copenhagen. In this position, he has led many cross-cutting reports and projects related to climate change impacts and adaptation in Europe. Most recently, he coordinated the first EU-wide climate risk assessment, which was published in March 2024. During his academic career, Füssel worked at the Potsdam Institute for Climate Impact Research, Stanford University, and Ritsumeikan University in Kyoto. He has consulted UNDP, UNFCCC, WHO, IPCC, the World Bank, the European Commission, and various national governments on climate change. He also served as author, review editor, reviewer, and member of government delegations for several IPCC Assessment Reports.

Sherri Goodman

Senior Fellow, Environmental Change & Security Program and Polar Institute, The Wilson Center

Sherri Goodman is an experienced leader and senior executive, lawyer, and director in the fields of national security, climate change, energy, science, oceans, and the environment. She is Secretary General of the International Military Council on Climate & Security; co-founder of Red Duke Strategies, a strategic advisory firm; Global Fellow at the Wilson Center's Polar Institute and Environmental Change & Security Program; and Senior Strategist at the Center for Climate and Security. Previously, she served as President and Chief Executive Officer of the Consortium for Ocean Leadership. Goodman also served as Senior Vice President and General Counsel of CNA, where she was also Founder and Executive Director of the CNA Military Advisory Board. As Chief Environmental, Safety, and Occupational Health Officer for the U.S. Department of Defense, she established relevant metrics for the department and led its Energy, Environmental, and Natural Resources Conservation programs.

Featured Speakers

Thushara Gunda
Complex Systems Analyst, Sandia National Laboratories

Thushara Gunda is a Principal Member of Technical Staff at Sandia National Laboratories. Her research portfolio focuses on data-driven decision making in complex systems, including water resources, energy, and security domains. Leveraging insights from interdisciplinary perspective is a key distinguishing feature of Gunda's work. Her research methods integrate techniques from data sciences, modeling and simulation, stakeholder engagement, open-source software development, and domain-specific practices.

Rossitza Homan
Manager, Resilience and Regulatory Effects Department, Sandia National Laboratories

Homan manages a diverse programmatic portfolio for the U.S. Department of Homeland Security and Department of Defense. She focuses on the risk and resilience of mission critical systems with particular focus on interdependent cyber-physical and social systems. For example, ICARUS examines anticipated impacts of climate change to inform adaptation options. Homan holds leadership positions across corporate initiatives and research portfolios at Sandia National Laboratories with a focus on mission-driven research, development, and applications for national security. Homan has held prominent technical leadership positions, including a Distinguished Member of Technical Staff special appointment. She has led multi-laboratory and international teams providing decision support to Lockheed Martin, the Department of Defense, the Department of Energy, and the Defense Advanced Research Projects Agency. Homan has taught at the University of Texas, led aerospace research and development at Bell Helicopter and Eclipse Aviation, and has worked at Sandia for 22 years.

Matthew Huber
David E. Ross Director of the Institute for a Sustainable Future, Purdue University

Matthew Huber is a professor in the Earth, Atmospheric, and Planetary Sciences Department at Purdue University and the inaugural David E. Ross Director of the Institute for a Sustainable Future, Purdue's transdisciplinary institute working on both fundamental and applied research in areas aligned with the United Nations Sustainable Development Goals. Huber's scholarship has been internationally recognized for its far-reaching global conclusions on Earth's habitability, resilience, and sustainability on long time horizons. His research areas include the physical processes generating tropical "thermostats," the polar amplification of warming, and the environmental, economic, ecological and evolutionary implications of these processes. Over the past decade, Huber' has shifted focus to emphasize more applied and solutions-oriented research to help society build a better future. Planning for future needs requires seeing energy, environment, economics, climate, health, politics and society as linked systems and considering risk, resiliency, and security in all of these areas concurrently.

David Johnson

Associate Professor of Industrial Engineering and Political Science, Purdue University

David R. Johnson is Associate Professor of Industrial Engineering and Political Science at Purdue University. He is the social science and policy lead in the Network Coordinating Office for the U.S. National Science Foundation's Natural Hazards Engineering Research Infrastructure, and a member of the U.S. Department of Homeland Security's Health, Food, and Agriculture Resilience Consortium. Johnson's interdisciplinary research focuses broadly on decision-making under uncertainty with applications in environmental policy, climate change mitigation and adaptation. Some of his key issues include coastal flood risk management, renewable energy policy, and water quality management. He is lead developer of the flood risk model used to assess the impacts of a wide range of flood protection systems for Louisiana's $50-billion Comprehensive Master Plan for a Sustainable Coast. Prior to joining Purdue, he worked for seven years as a policy analyst and mathematician at RAND Corporation.

Rob Leland

Climate Change Security Center Director, Sandia National Laboratories

Rob Leland is the Director of the Climate Change Security Center at Sandia National Laboratories. He leads climate strategy development across the Labs, directs the Earth Sciences Research Foundation, and oversees laboratory and field work in New Mexico, Texas, and Alaska. Leland joined Sandia in 1990 as a high-performance computer researcher and has served as the director of computing research, Vice President for Science and Technology, and Chief Technology Officer. In 2014, he worked at the White House Office of Science and Technology Policy leading development of the National Strategic Computing Initiative to sustain U.S. leadership in supercomputing. In 2017, Leland became Associate Laboratory Director for Scientific Computing and Energy Analysis at the National Renewable Energy Laboratory. He returned to Sandia in 2021.

Piret Pernik

Researcher, Strategy Branch of the NATO Cooperative Cyber Defence Centre for Excellence

Piret Pernik is a researcher at the Strategy Branch of the NATO Cooperative Cyber Defence Centre for Excellence. Her main research interests are cybersecurity strategies and policies, cyber defence and military cyber forces, as well as cybersecurity and national security implications of emerging and disruptive technologies, including artificial intelligence and machine learning, cybersecurity of next-generation mobile networks (5G and beyond), and cybersecurity and cyberspace domain operations in the multidomain. She has authored and co-authored numerous reports and policy analyses. Prior to joining the CCDCOE in 2019, Pernik was a Research Fellow at the International Centre for Security and Defence, Estonia's largest think-tank focused on security and defence matters. She worked as a Researcher at the Estonian Academy of Social Sciences. Between 2003 and 2013, she served in the Estonian Ministry of Defence and was an adviser of the National Defence Committee of the Parliament of Estonia.

Featured Speakers

Eyüp Turmuş
SPS Advisor and Programme Manager, NATO Innovation, Hybrid and Cyber Division

Eyüp Turmuş is the advisor and program manager for the NATO Science for Peace and Security Programme, part of the NATO Innovation, Hybrid and Cyber Division. In this role, he contributes to NATO's work to address security challenges, crisis management, and disaster response. He oversees research and capacity-building activities with NATO's partners in various locations worldwide, focusing on emerging and disruptive technologies.

Sunny Wescott
Chief Meteorologist, U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency

Sunny Wescott is a Lead Meteorologist specializing in national extreme weather hazards and climatological studies for impacts to public and private sector key resources. During her time in the U.S. Air Force as a Lead Meteorologist, Wescott trained on continental and oceanic weather as the Top Forecaster for her support region and is considered a subject matter expert for multiple climatological events such as drought, subsidence, wildfires, tropical cyclones, and winter storms. Her previous roles within CISA were working with emergency response operations for Telecommunications and Critical Infrastructure which integrated her background with mission support forecasting from her military experience. Her current role as CISA's Extreme Weather Outreach lead for the Infrastructure Security Division enables her to provide focused climate reports for regions and critical infrastructure operators.

Lynn Yang
Manager, Cybersecurity Systems Analysis, Sandia National Laboratories

Lynn Yang leads a systems research and analysis group at Sandia National Labs, California, which focuses on national security issues, including climate change, integrated deterrence, and cyber and infrastructure security. She has worked on critical infrastructure risk analysis projects for the U.S. Department of Homeland Security, Department of Defense, and other federal departments and agencies for two decades. Yang has helped develop models and conducted risk-based analyses of infrastructure impacts due to man-made and natural disasters. Currently, she leads a portfolio that includes climate security projects stemming from Sandia's Climate Security Strategy, a National Nuclear Security Agency Strategic Outlook Initiative on climate impacts to NNSA missions, cybersecurity projects, and experimental wargaming projects.

Attendees

Rebecca Adler Miserendino
Principal
Lewis-Burke Associates
rebecca@lewis-burke.com

Amir AghaKouchak
Chancellor's Professor, Department of Civil & Environmental Engineering
University of California, Irvine
amir.a@uci.edu

Lilian Alessa
President's Professor and Co-Director, The Center for Resilient Communities
University of Idaho
alessa@uidaho.edu

David Alexander
Senior Science Advisor for Resilience
U.S. Department of Homeland Security S&T
david.alexander1@hq.dhs.gov

Jeffrey Allen
International Cooperative Programs Office
U.S. Department of Homeland Security S&T
jeffrey.allen@hq.dhs.gov

Cristal Armijo
Climate Change Policy Analyst
NATO Allied Command Transformation
cristal.armijo@act.nato.int

Jeffrey Arnold
Chief Scientist for Climate and Environmental Sciences
MITRE Corporation
jarnold@mitre.org

Anjuli Bamzai
Senior Science Advisor
U.S. National Science Foundation GEO
abamzai@nsf.gov

Guy Barnett
Principal Research Consultant
CSIRO
guy.barnett@csiro.au

David Batz
Managing Director, Cyber & Infrastructure Security
Edison Electric Institute
dbatz@eei.org

Alfred Bender
Deputy Director for Risk Policy
U.S. Department of Homeland Security
alfred.bender@hq.dhs.gov

Budhendra (Budhu) Bhaduri
Director of Science, Programs and Partnerships, National Security Sciences
Oak Ridge National Laboratory
bhaduribl@ornl.gov

Alex Blauensteiner
BD&C Manager
CSIRO
alex.blauensteiner@csiro.au

Ben Bonin
Principal Member of the Technical Staff/Systems Analysis
Sandia National Laboratories
bjbonin@sandia.gov

Jonathan Bransky
Director Threat Intelligence
Dominion Energy
jonathan.s.bransky@dominionenergy.com

Stacey Connaughton
Director, The Purdue Policy Research Institute
Purdue University
sconnaug@purdue.edu

Daniel Cotter
Executive Director
U.S. Department of Homeland Security OSE
daniel.cotter@hq.dhs.gov

Bradley Dean
Director for Flood & Resilience Policy
Council on Environmental Quality, Executive Office of the President
bradley.j.dean@ceq.eop.gov

William (Bill) DeLong
Regional Resiliency Assessment Program Coordinator
U.S. Department of Homeland Security CISA
william.delong@cisa.dhs.gov

Amanda Dodd
Director, Computation and Analysis for National Security Center
Sandia National Laboratories
ajbarra@sandia.gov

Tom Ellison
Deputy Director
Center for Climate & Security
tellison@csrisks.org

Mark Flood
Senior Research Scholar, Center for Financial Policy
University of Maryland
mdflood@umd.edu

Giovanni Fusina
Defence Scientist, Centre for Security Science
Defence Research and Development Canada/ Government of Canada
giovanni.fusina@forces.gc.ca

Hans-Martin Füssel
Coordinator
European Climate Risk Assessment
hans-martin.fuessel@eea.europa.eu

Matteo Gerlini
Assistant Professor
University of Siena
matteo.gerlini@unisi.it

Sherri Goodman
Senior Fellow, Environmental Change & Security Program and Polar Institute
Wilson Center
Sherri.Goodman@wilsoncenter.org

Marthie Grobler
Principal Research Scientist
CSIRO
marthie.grobler@data61.csiro.au

Thushara Gunda
Complex Systems Analyst
Sandia National Laboratories
tgunda@sandia.gov

Diana Hackenburg
Climate Security Communications
Sandia National Laboratories
dmhacke@sandia.gov

Nick Heavens
Climate Modelling Intrapreneur
Viridien
nick.heavens@cgg.com

Rossitza Homan
Manager, Resilience and Regulatory Effects Department
Sandia National Laboratories
rhoman@sandia.gov

Matthew Huber
David E. Ross Director, Institute for a Sustainable Future
Purdue University
huberm@purdue.edu

Hengameh Irandoust
Scientist
NATO Cimate Change and Security Centre of Excellence
hengameh.irandoust@ccascoe.org

Nicole Jackson
Senior Member of the Technical Staff
Sandia National Laboratories
njacks@sandia.gov

Helge Janicke
Research Director
Cyber Security Cooperative Research Centre
helge.janicke@cybersecuritycrc.org.au

Jonas Johansson
Associate Professor in Critical Infrastructure at the Division of Risk Management and Societal Safety
Lund University
jonas.johansson@risk.lth.se

David Johnson
Associate Professor in Industrial Engineering & Political Science
Purdue University
davidjohnson@purdue.edu

Tim Judge
Senior Vice President, Head of Modeling & Chief Climate Officer
Fannie Mae
timothy.judge@fanniemae.com

Christina Karamperidou
Professor Department of Atmospheric Sciences
University of Hawai'i at Mānoa
ckaramp@hawaii.edu

David Kaufman
Vice President for Safety and Security
Center for Naval Analyses
kaufmand@cna.org

Robert Kopp
Director, Megalopolitan Coastal Transformation Hub
Rutgers University
robert.kopp@rutgers.edu

Stephanie Kuzio
Manager, Energy Water System Integration
Sandia National Laboratories
spkuzio@sandia.gov

Rob Leland
Director, Climate Change Security Center
Sandia National Laboratories
leland@sandia.gov

Igor Linkov
Senior Scientific Technical Manager
U.S. Army Engineer Research and Development Center

Richard Matear
Chief Research Scientist, Climate Science Centre
CSIRO Oceans and Atmosphere, Hobart
richard.matear@csiro.au

Mike McDonald
President & Co-founder
Global Resilience Initiatives Inc.
michael.d.mcdonald@mac.com

Crystall Merlino
Director, Resilience, Energy & Sustainability Program
U.S. Department of Homeland Security
crystall.merlino@hq.dhs.gov

Malcolm Mistry
Researcher and Lecturer
Climate Change, Energy and Adaptation, Ca' Foscari University of Venice, Italy
Assistant Professor in Climate and Geo-Spatial Modelling
Environment & Health Modelling Lab, Department of Public Health, Environments and Society at The London School of Hygiene & Tropical Medicine, UK
malcolm.mistry@unive.it

Nuno Mota
Economist
Fannie Mae
Nuno_Mota@fanniemae.com

David Mussington
Executive Assistant Director for Infrastructure Security
U.S. Department of Homeland Security CISA
bmussing@umd.edu

Candace Nachman
Senior Ocean Policy & Program Advisor
U.S. Coast Guard
candace.a.nachman@uscg.mil

Noël Nachtigal
Senior Scientist
Sandia National Laboratories
nmnacht@sandia.gov

Marcin Niemiec
Professor
AGH University of Science and Technology Stanisław Staszic in Krakow Institute of Telecommunications
marcin.niemiec@agh.edu.pl

Irene "Tesha" Okioga
Director of Engineering Services
Western Virginia Water Authority
irene.okioga@westernvawater.org

Ken Patel
Manager, Purdue University Partnerships
Sandia National Laboratories
kdpatel@sandia.gov

Piret Pernik
Researcher Strategy Branch
NATO Cooperative Cyber Defence Centre of Excellence
piret.pernik@ccdcoe.org

Markus Pohlman
Senior Counsel, Environment & International Law (LEGEN)
World Bank
mpohlmann@worldbank.org

Leslie Proctor
Business Development Specialist
Sandia National Laboratories
lprocto@sandia.gov

Giovanni Russello
Head, School of Computer Science
Auckland University
g.russello@auckland.ac.nz

Adam Rutherford
Climate Change and Security (Futures) lead
NATO ACT
Adam.rutherford@act.nato.int

Honor Sangster
Infrastructure Policy Advisor
UK Ministry of Defence
honor.sangster100@mod.gov.uk

Merideth Secor
Branch Chief at the National Risk Management Center
U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency
merideth.secor@cisa.dhs.gov

Vishal Sharma
Program Director
U.S. National Science Foundation CISE
vsharma@nsf.gov

Frantisek Simancik
Member of The Presidium of SAS
Slovak Academy of Sciences
simancik@up.upsav.sk

Gavril Torrijos
Associate
Zeichner Risk Analytics
gtorrijos@zra.com

Zachary Smith
Senior Technical Advisor for Data & Analytics
U.S. Department of Homeland Security FEMA
zachary.smith@fema.dhs.gov

Benjamin Trump
Senior Research Social Scientist
U.S. Army Engineer Research and Development Center

Eyüp Turmuş
SPS Advisor and Programme Manager
NATO Innovation, Hybrid and Cyber Division
turmus.eyup@hq.nato.int

Swathi Veeravalli
Director for Climate Security and Adaptation
National Security Council
swathi.veeravalli@nsc.eop.gov

Gernot Wagner
Climate Economist
Columbia Business School
gernot@gwagner.com

Shannon Walsh
Strategic Research Consultant
Zeichner Risk Analytics
swalsh@zra.com

Sunny Wescott
Chief Meteorologist
U.S. Department of Homeland Security CISA
sunny.wescott@cisa.dhs.gov

Kellee Wicker
Director, Science and Technology Innovation Program
Wilson Center
kellee.wicker@wilsoncenter.org

Nick Winstead
Vice President
Zeichner Risk Analytics
nick@zra.com

Kristin Wyckoff
Senior Advisor for Strategic Foresight & Futures
U.S. Department of Homeland Security S&T
kristin.wyckoff@hq.dhs.gov

Dongyan Xu
Samuel Conte Professor of Computer Science, Director of CERIAS
Purdue University
dxu@purdue.edu

Lynn Yang
Manager, Cybersecurity Systems Analysis
Sandia National Laboratories
liyang@sandia.gov

Briefing: Unravelling the Cyber-Physical-Social Infrastructure Climate Change (CPSICC) Nexus

Climate change and cybersecurity threats are converging as interconnected risks, presenting challenges to global security, infrastructure, and societal well-being. The accelerating impacts of climate change magnify vulnerabilities in critical infrastructure that are increasingly dependent on digital technologies. Sophisticated cyber threats can target the very technologies designed to improve efficiency and resilience. Simultaneously, cyber-attacks can destabilize systems already weakened by environmental stressors. This creates a vicious cycle of escalating risks, where the impacts of climate change and cyber threats are mutually reinforcing and amplifying the overall threat landscape.

In this interconnected world, the ramifications of these combined environmental and cyber threats extend beyond immediate physical damages. They pose significant economic risks, threatening global trade, financial stability, and corporate operations. Politically, they can undermine public trust in government and institutions, fuel social unrest, and contribute to geopolitical tensions. Socially, they affect public health, safety, and community resilience, with the most vulnerable populations bearing the brunt of these impacts. To address these challenges, it is imperative to develop integrated strategies that enhance the resilience of critical infrastructures, improve cybersecurity measures, and foster global cooperation. By understanding and addressing the nexus between climate change and cybersecurity, we can better protect our societies and ensure a more secure and sustainable future.
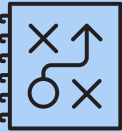
Why is this a problem?

The accelerating impacts of climate change, including more frequent and severe weather events, rising sea levels, and shifting climate patterns, magnify vulnerabilities in critical infrastructure. These infrastructures, such as energy grids, water supply systems, and transportation networks, are increasingly dependent on digital technologies for their operation and management. This increased digitization exposes more devices and systems to potential cyber-attacks, which are further exacerbated by climate-induced disruptions such as extreme weather events. Cyber-attacks can inflict significant environmental damage, disrupt vital climate monitoring services, and undermine efforts to mitigate and adapt to climate change.

For example, a cyber-attack on a power grid during a heatwave could result in widespread blackouts, leaving millions without air conditioning and heightening the risk of heat-related illnesses. Similarly, an attack on water treatment facilities during a flood could contaminate water supplies, leading to a public health crisis. The interconnected nature of modern infrastructure means that an attack on one system can trigger cascading failures across multiple sectors, leading to widespread economic disruption, political instability, and social unrest. Addressing these compounded threats requires integrated strategies, robust infrastructure, and coordinated global efforts to enhance resilience and security.

What do we aim to achieve with CPSICC?

The goal of CPSICC (Cyber-Physical-Social Infrastructure Climate Change) is to develop integrated strategies that enhance the resilience of critical infrastructures against the compounded threats of climate change and cyber-attacks. By fostering collaboration across sectors, improving public awareness and preparedness, investing in resilient infrastructure, and developing adaptive policy frameworks, CPSICC aims to safeguard social well-being, ensure the continuity of essential services, and mitigate the risks posed by these dual threats.

Key themes and impacts:

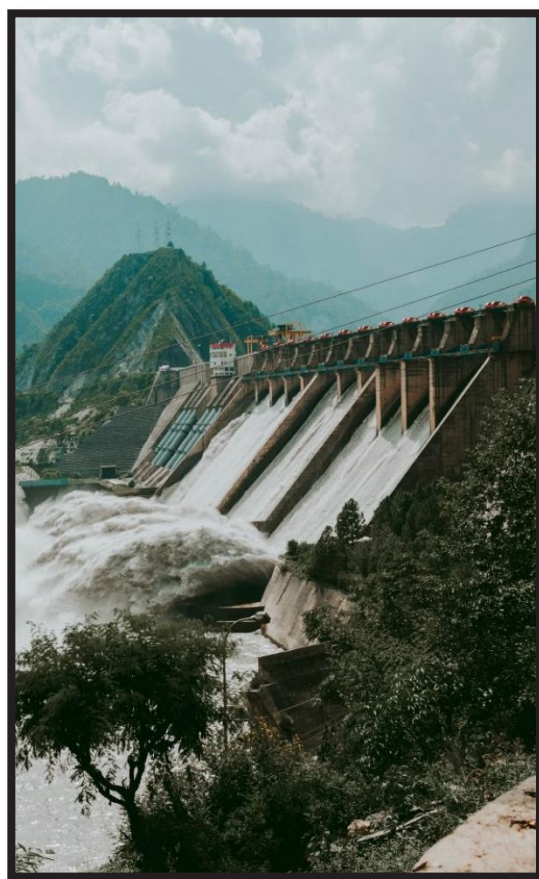|	
	Climate change and cybersecurity — Both climate change and cyber threats significantly impact the safety and functioning of critical infrastructure. — Increased digitization within critical infrastructure sectors increases vulnerability to cyber-attacks, which can be exacerbated during climate-related disruptions.
	Critical infrastructure interdependencies — Climate change and cyber-attacks threaten critical infrastructure systems, impacting water, energy, and food security, critical for societal functions. — The rapid digitization of critical infrastructure can help mitigate climate risks but also increase susceptibility to cyber-attacks. — Due to the interdependencies of critical infrastructure systems, climate change and cyber-attacks can compound and/or cascade, triggering cascading failures across multiple sectors.
	Social, economic and geopolitical impacts — Climate change and cyber threats influence public health, safety, social stability, and community resilience. — Extreme weather events and cyber-attacks can lead to community displacement, exacerbate resource scarcity, and widen the digital divide, impacting social and economic inequalities. Both threats disproportionately affect vulnerable populations, exacerbating economic disparities and vulnerabilities. — Geopolitical tensions arise from resource competition, cyber espionage, and warfare, necessitating coordinated international policies and cooperation.
	Data forecasting and prediction services — Climate change and cyber threats impact the accuracy and reliability of forecasting and prediction services, essential for public safety and economic stability. — Climate change and cyber threats disrupt global trade, affect critical industries like energy and agriculture, and pose risks to financial system stability. — Cyber-attacks can disrupt critical climate monitoring services and directly cause environmental damage, hindering efforts to address climate change.
	Investing in resilience and mitigation — Addressing the nexus between climate change and cybersecurity requires coordinated efforts across policy, technology, and business practices. — Cyber-attacks on critical infrastructure and climate-induced instability pose significant national security threats.

Climate change and cyber threats

The interconnectedness of climate change and cybersecurity presents emerging risks to global security. This is because the resilience and security of critical infrastructure are vital for national security, economic stability, and societal well-being. As infrastructure systems become increasingly digitized, they face heightened vulnerabilities from both cyber threats and climate change. This section provides examples of climate and/or cyber threats to critical infrastructure.

Both climate change and cyber threats significantly threaten the safety and security of critical infrastructure. The increased digitization of critical infrastructure systems increases its exposure to potential cyber-attacks, which can be further exacerbated by climate-related disruptions. This theme provides examples of how climate change and cybersecurity individually and/or collectively might threaten key critical infrastructure such as water, energy and food sectors.

Water sector

Climate change threatens **water security**[1] through impacts on the water cycle by influencing when, where, and how much precipitation falls. It also leads to more severe weather events over time, impacting the availability and quality of freshwater supplies. For example, an increase in flood events increases the runoff of contaminants such as fertilizers, polluting the water supply and limiting access to safe water for humans and the ecosystem. The rising sea levels also contaminates underground freshwater with salt water. Droughts decrease the availability of water for human consumption as well as for energy and food production.

Cyber-attacks also threaten water security. For example, a cyber-attack targeting the water treatment system in Oldsmar, Florida, in 2021[2], involved an attempt to increase the levels of sodium hydroxide (lye) in the water supply to dangerous levels. Although the attack was thwarted before any harm was done, it highlighted the potential for cyber breaches to cause serious environmental and public health consequences by contaminating water supplies. Another example dates to 2001, when an insider attack led to a sustained cyber-attack against the Maroochy Shire's sewage control, seeing 265,000 gallons of untreated sewage flowing into local parks and rivers, causing significant damage to the local environment[3].

---

[1] https://education.nationalgeographic.org/resource/how-climate-change-impacts-water-access/

[2] https://edition.cnn.com/2021/02/08/us/oldsmar-florida-hack-water-poison/index.html

[3] https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-an-insider-releases-265000-gallons-of-sewage-on-the-maroochy-shire/

Energy sector

Both climate change and cyber threats pose significant risks to **energy security**. On the supply side, extreme weather events can impact the generation of renewable energy, as well as energy transmission and distribution. For example, extreme heat can lower solar power cell efficiency; wildfires and/or cyclones can damage wind and solar energy infrastructure; drought can reduce water availability for hydropower; wildfires, floods and/or tropical storms can damage transmission infrastructure such as transmission towers and/or power poles. On the demand side, heat waves are a major driver of customer electricity demand, increasing the risks of power outages[4]. Extreme conditions like high winds and ice storms could strain and physically damage critical infrastructure such as energy grids and communication networks. A cyber-attack during winter could lead to prolonged power outages, leaving communities without heat and light, and posing serious health risks. Disrupted communication networks could hinder emergency responses to natural disasters. The combination of severe weather and logistical challenges in vulnerable regions such as the Arctic highlights the need for robust cybersecurity and resilient infrastructure. The energy transition is also changing the energy system vulnerability profile as a result of increasing electrification and digitalization of the energy system. Digital technologies enhance efficiency and control but also open new avenues for cyber threats.

Several instances of extreme weather events or cyber-attacks have disrupted the energy system. For example, in April 2022, three German wind energy companies were hit with cyber-attacks that disabled thousands of digitally managed wind turbines[5]. In 2021, the Texas power grid failure left millions without electricity[6] and in 2020 SolarWinds cyber-attack affected numerous organizations globally[7]. In 2015, a cyber-attack on the western Ukraine power grid impacted the distribution of electricity. In this attack, hackers gained access to the control systems of three energy distribution companies, causing widespread blackouts that affected approximately 230,000 people. This incident highlighted the vulnerability of critical infrastructure to sophisticated cyber-attacks, demonstrating the need for robust cybersecurity measures in the face of increasing digitization[8] [9] [10].

---

[4] ESCI Project Final Report, Available at https://climatechangeinaustralia.gov.au/en/projects/esci/esci-publications/esci-project-reports/

[5] https://www.securityweek.com/german-wind-turbine-firm-discloses-targeted-professional-cyberattack/

[6] https://earth.org/texas-energy-crisis-why-is-the-states-power-grid-so-fragile/

[7] https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

[8] Defense Use Case. "Analysis of the cyber attack on the Ukrainian power grid." Electricity information sharing and analysis center (E-ISAC) 388.1-29 (2016): 3.

[9] https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802

[10] https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine

Food sector

Climate change also threatens **food security** through impacts on the productivity of agricultural and fishery sectors, biosecurity and food safety, animal and human health and wellbeing, as well as farming livelihoods[11]. For example, climate change impacts the productivity of animal feedstock such as corn. A study forecasts a 20-40% decline in U.S. corn belt production from 1991-2000 levels by 2046-2055[12]. Increased extreme high temperatures will also lower livestock productivity due to heat stress, increased likelihood of disease, lower animal feed efficiency and reproductive health. Higher temperatures will also demand more water to maintain animal health and well-being, putting additional pressure on water security. The impact of climate change on meat supply chains leads to meat shortages and price increases, which increases food inequity.

One strategy that helps minimise climate change risks to agriculture is digital-based technologies (e.g., robotics, aerial imaging, digital mapping of seeds, and GPS). This is because digital agriculture can increase resource efficiency, improve access to climate forecasting and help minimise the impact of climate change on food production. However, the digitalization of agriculture and food production also increases exposure to cyber-attacks[13]. It is therefore no surprise that the threat of cyber-attacks on food safety and the food supply chain is growing. For example, in June 2021, the world's largest meat processing company, JBS Foods, paid eleven million dollars in ransom to resolve a cyber-attack that halted their U.S. cattle slaughtering for a day[14]. Cyber-attacks targeting agricultural data and automated systems can exacerbate climate risks, further impacting food security.

NATO's approach to climate change is informed by two foundational documents: the NATO Climate Change and Security Action Plan[15] and the 2022 Strategic Concept[16]. Because NATO decisions require consensus, the adoption of these documents represented a paradigmatic shift in the alliance's outlook on climate change. NATO describes climate change as a crisis and threat multiplier and consistently identifies three priorities: improving understanding of climate change and security, adapting to climate change, and contributing to climate change actions. NATO assesses that climate change will multiply

---

[11] Nature Climate Change 2024 Vol. 14 Issue 3 Pages 207-207. DOI: 10.1038/s41558-024-01970-y

[12] https://www.weforum.org/agenda/2024/01/food-system-impact-of-climate-change/

[13] https://www.usaid.gov/digital-development/cybersecurity/agriculture-food-security-briefer

[14] https://www.cfr.org/blog/digital-agriculture-gap-critical-infrastructure-protection

[15] https://www.nato.int/cps/en/natohq/official_texts_185174.htm

[16] https://www.nato.int/cps/en/natohq/topics_210907.htm

threats by increasing natural hazards, competition over resources, state fragility, migration events, and conflicts. The increase of these threats will stretch the capacity of NATO forces. Climate change will adversely impact NATO members' critical infrastructure, military installations, assets, personnel, and operations in all domains. NATO seeks to strengthen national and international resilience to prepare for these impacts.

Critical infrastructure interdependencies

Hazard events threatening critical infrastructure are increasingly interconnected, leading to a compounding effect where one hazard triggers another and creates a cascading impact. Climate and cyber risks are exacerbated by the degree and extent of interdependence between and across critical infrastructure sectors and the potential for cascading and/or compounding effects. This section highlights some of the interdependencies existing between critical infrastructure sectors.

Critical infrastructure interdependencies refer to the interconnectedness and reliance among different essential systems, assets and networks. These interdependencies mean that the functioning of one sector (such as energy, water, transportation, telecommunications, or financial services) often depends on the functioning of others. Disruptions in one infrastructure can cascade and impact multiple other sectors, highlighting the need for comprehensive risk management and coordinated protection strategies to ensure overall resilience and stability. Critical infrastructure interdependencies significantly influence the protection and resilience of these assets by creating complex vulnerabilities and cascading risks that require coordinated and holistic strategies to manage.

Due to the interconnectedness of critical infrastructure systems, there is a need for an improved systems understanding of socio-technical-economic interdependencies in the design, operation and adaptation of critical infrastructure that considers potential chain reactions[17]. The interdependencies of the sectors are critical to improving the resilience of the system as a whole and avoiding maladaptation. For example, understanding drought impacts might require an understanding of the needs of multiple sectors (e.g., food and energy) as well as implications to the supply chain (e.g., food distribution), health (e.g., risk of increased infectious disease) and ecosystem (e.g., longer-term animal migration). Similarly, investments that aim to mitigate carbon emissions (e.g., clean hydrogen) could require additional water investments that could ultimately influence supply chain and trade dynamics.

Any disruptions to critical infrastructure would have cascading impacts on supply chains and access and/or availability to other critical infrastructure such as health, medical and emergency services, provision and supply of food and the functioning of defence forces[18]. The interdependency of telecommunications with energy; and telecommunications and data storage with the financial services, health and transport sectors and the extension into essential services such as medical supplies, childcare, aged care, retail banking, and freight movement are a good example. In November 2023, Australia's second-largest telecommunications company, Optus, were affected by mobile phone and internet services outages, affecting 10 million customers and cascading to impact many more. This outage impacted 400,000 businesses; government departments; health and transport systems in

---

[17] https://link.springer.com/content/pdf/10.1007/978-3-642-45330-4_12.pdf

[18] Lawrence, J., Blackett, P., & Cradock-Henry, N. A. (2020). Cascading climate change impacts and implications. Climate Risk Management, 29, 100234. https://doi.org/https://doi.org/10.1016/j.crm.2020.100234

Melbourne; and health and water services in South Australia. It is estimated this event cost the Australian economy AU$1 billion[19].

Several examples real-world examples exist to illustrate these interdependencies:

- In countries such as the UK where half of the food supply is imported (e.g., 80% of fruit, 50% of vegetables, and 20% of beef and poultry), any impacts due to climate and cyber security threats will lead to greater **food (in)security** exposure of interdependencies on global food supply chains. Disruptions to food imports and supply chains due to climate disasters and/or cyber threats in the countries that supply food to the UK can have a significant impact on the UK's food availability. A fall in the availability of food tends to lead to rising prices, which increases the risk of social unrest[20].
- **Water security** is critical to both ecosystems and human society as water availability impacts local topography, and animal migration, provides drinking water and sanitation needs for animal and human health as well and enables the production of energy, food and manufactured goods essential for basic human needs, impacting multiple systems.
- **Food security** can be threatened by cascading effects originating from the disruption to other sectors such as electricity, communication and transport which can impact both on-farm and off-farm supply chain infrastructure. In the East Kimberley, a remote region of Western Australia, food security was threatened by the disruption of transport routes that prevented trucks from delivering food supplies in 2023. Such disruption, which originated in the transport system, had cascading effects on the food systems and the defence forces, which were called upon to assist in supplying food during the disruption[21].
- **Energy security** can be impacted by an extreme weather event and/or cyber-attack on energy infrastructure that can lead to widespread blackouts and affect other critical services such as healthcare, transportation, supply chain, and communication. More specifically, power outages might impact mobile phone coverage, access to safe water for consumption and wastewater treatment, and access to fuel, transport and banking facilities to pay for basic necessities. It also impacts access to appropriate indoor temperatures (e.g., heating and cooling systems), life support equipment and/or storage of fresh food and medication impacting human health and wellbeing.
- **Supply chain security** can also be impacted due to liquid fuel supply issues. For example, in May 2021, nearly half of the U.S. East Coast's fuel supply was shut down after a cyber-attack forced Colonial Pipeline to shut its entire network, causing fuel prices to spike ahead of peak U.S. summer driving season, negatively impacting consumers and the economy[22] [23].
- Another example illustrates how cyber-attacks on steel production can have cascading impacts and can cause **environmental damage**[24]. For instance, a 2015 cyber-attack on a German steel plant disrupted production controls. This incident resulted in significant physical damage to the plant, releasing pollutants into the environment and causing a substantial increase in emissions due to the improper handling of materials during the disruption.

---

[19] https://www.abc.net.au/news/2023-11-08/optus-outage-mobile-phones-internet-what-happened/103077180
[20] https://theconversation.com/climate-change-could-lead-to-food-related-civil-unrest-in-uk-within-50-years-say-experts-214754
[21] https://www.abc.net.au/news/2023-03-08/defence-force-to-aid-food-shortage-in-flooded-east-kimberley/102068096
[22] https://www.weforum.org/agenda/2021/05/cyber-attack-on-the-us-major-oil-and-gas-pipeline-what-it-means-for-cybersecurity/
[23] https://www.bbc.com/news/business-57050690
[24] https://www.bbc.com/news/technology-30575104

Social, economic and geopolitical impacts

Climate change and cybersecurity threats have profound social, economic and geopolitical impacts. For example, it might impact public health and safety, community resilience and social cohesion as well as global trade and financial stability. It may also destabilize governments, alter geopolitical landscapes, and impact international relations. Integrated strategies and coordinated policies are critical to safeguard social well-being, economic resilience and stability as well as international cooperation. This section highlights some of these impacts.

Social impacts

Climate events and cyber-attacks on critical infrastructure, such as water and healthcare systems, can severely disrupt services essential for **public health and safety**. For instance, cyber-attacks on water supply systems can lead to contamination or disruption of water services, posing significant health risks to communities. Climate change increases the frequency and severity of extreme weather events such as heatwaves, floods, and hurricanes. These events can have direct health impacts, causing injuries, heat-related illnesses, and stress on healthcare systems. Indirect impacts include the spread of infectious diseases and compromised access to clean water and food[25].

Climate change exacerbates resource scarcity, leading to competition over essential resources like water and arable land. This can increase **social tensions and conflict** within and between communities, impacting social cohesion. For example, in the Lake Chad Basin, the effects of climate change have significantly reduced the size of Lake Chad, which is a critical water source for Nigeria, Chad, Cameroon, and Niger[26]. This reduction has led to heightened competition over water and arable land, exacerbating existing conflicts and contributing to the rise of militant groups like Boko Haram. The resulting social instability highlights the need for integrated resource management and conflict resolution strategies to enhance community resilience in the face of climate-induced resource scarcity.

Extreme weather events and sea-level rise can also force communities to relocate, leading to **social displacement** and the loss of homes and livelihoods. Cyber-attacks that disrupt essential services during such crises can further aggravate the situation, making recovery and adaptation more challenging. For example, in 2017, Hurricane Maria devastated Puerto Rico, causing widespread displacement[27]. The island's power grid was severely damaged, and a subsequent cyber-attack on the Puerto Rican Electric Power Authority (PREPA) further delayed power restoration. This compounded the crisis, making recovery more challenging for affected communities. This highlights the need for resilient infrastructure and robust cybersecurity to support communities during extreme weather events.

Both climate change and cyber threats disproportionately affect **vulnerable populations**, including low-income communities, the elderly, and those with pre-existing health conditions[28]. These groups often lack the resources and capabilities to effectively respond to and recover from such threats. The increasing reliance on digital solutions for climate adaptation and response highlights the digital divide.

---

[25] https://www.who.int/news-room/fact-sheets/detail/climate-change-and-health
[26] https://www.msf.org/lake-chad-crisis-depth
[27] https://www.sciencedirect.com/science/article/pii/S2212420919311847
[28] Benevolenza, M. A., & DeRigne, L. (2018). The impact of climate change and natural disasters on vulnerable populations: A systematic review of literature. Journal of Human Behavior in the Social Environment, 29(2), 266–281. https://doi.org/10.1080/10911359.2018.1527739

Communities without adequate access to technology and internet services are at a disadvantage, exacerbating existing social and economic inequalities[29].

Economic impacts

Climate events and cyber-attacks on critical infrastructure can have significant economic impacts. Rising sea levels, more frequent and severe hurricanes, and changes in precipitation patterns can **disrupt global trade routes** and port operations, affecting the global supply chain. Major port cities are particularly vulnerable to these disruptions, which can lead to significant economic losses[30]. Cyber-attacks on logistics and transportation infrastructure can also impact global supply chains. For example, a 2017 ransomware attack on Maersk, a leading shipping company, caused severe disruptions[31]. The attack led to a complete shutdown of Maersk's IT systems, halting operations across 76 ports worldwide. This incident resulted in significant delays in shipping schedules and supply chain disruptions. The financial impact was substantial, with Maersk reporting losses of up to $300 million (USD) due to the attack. Similarly, the NotPetya malware attack, which affected several industries including logistics, resulted in global economic damages estimated at $10 billion (USD). Companies such as FedEx and pharmaceutical giant Merck also reported losses in the hundreds of millions due to disrupted operations and recovery costs[32].

Increasingly, financial institutions must account for climate-related risks such as property damage from extreme weather and investment losses in fossil fuel industries. These risks affect asset values and increase the **volatility of financial markets**. In addition, financial institutions are prime targets for cyber-attacks, which can result in direct financial loss, data breaches, and erosion of customer trust. The integration of robust cybersecurity measures is essential to protect financial stability. For example, JPMorgan Chase, a leading global financial institution, has implemented comprehensive cybersecurity measures to protect its operations. Following a major data breach in 2014, where the personal information of 76 million households and 7 million small businesses was compromised, JPMorgan Chase invested heavily in bolstering its cybersecurity defences. The bank allocated $600 million (USD) annually to cybersecurity and employed a team of over 3,000 IT security professionals. By adopting advanced security protocols, establishing a robust security operations center, and engaging in continuous employee training, JPMorgan Chase has significantly enhanced its ability to defend against cyber threats, ensuring the security and resilience of its critical infrastructure[33].

Political and geopolitical impacts

Cyber-attacks on critical infrastructure, highlight the potential for significant **national security threats**, with anticipated adverse impacts on military assets, infrastructure, and operations. For example, the 2017 cyber-attack on the Ukrainian power grid[34], which came on the heels of the initial 2015 attack, further demonstrated the geopolitical realities of such threats. This attack temporarily disrupted power to Kiev, affecting hundreds of thousands of residents. It was widely attributed to a state-sponsored hacking group, underlining the role of cyber-attacks as tools of geopolitical strategy. These attacks can disrupt

---

[29] Dargin, J. S., Fan, C., & Mostafavi, A. (2021). Vulnerable populations and social media use in disasters: Uncovering the digital divide in three major U.S. hurricanes. International Journal of Disaster Risk Reduction, 54, 102043. https://doi.org/https://doi.org/10.1016/j.ijdrr.2021.102043

[30] https://science.nasa.gov/climate-change/effects/

[31] https://www.bbc.com/news/technology-40416611

[32] https://www.cbsnews.com/news/lessons-to-learn-from-devastating-notpetya-cyberattack-wired-investigation

[33] https://www.ft.com/content/cd287352-cb3b-48d8-a85b-668713b80962

[34] https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

essential services, undermine public trust, and create political instability. Climate change exacerbates existing vulnerabilities and can lead to resource scarcity, forced migration, and conflict. These conditions create opportunities for cyber-attacks, further destabilizing regions.

Climate change contributes to societal unrest, leading to increased activism both offline and online. 'Hacktivism'—hacking for political or social causes—has risen as a method to draw attention to climate issues, with activists using cyber-attacks to further their agendas. Climate change intensifies competition for natural resources, such as water and arable land. This competition can lead to **geopolitical tensions and conflicts**, particularly in regions already prone to instability. Nations may use cyber capabilities to gain strategic advantages in resource competition and political influence. Cyber espionage involves the covert acquisition of confidential information from other nations, including intellectual property, government secrets, and strategic plans. For example, the cyber-espionage group APT29[35], believed to be linked to a nation-state, conducted extensive campaigns targeting government agencies and industries to steal sensitive data, enhancing its competitive position in global markets. A more recent example includes Volt Typhoon, a state-sponsored actor that typically focuses on cyber disruption and information gathering, with the intent to disrupt communications infrastructure in the Pacific[36]. Cyber warfare is another attack vector that involves aggressive tactics such as disrupting critical infrastructure, manipulating data, and spreading misinformation to destabilize opponents. A notable example is the Stuxnet worm, which targeted Iran's nuclear program in 2010, allegedly developed by the United States and Israel[37]. This sophisticated cyber weapon disrupted Iran's uranium enrichment process, setting back its nuclear capabilities.

Current governance frameworks often treat cybersecurity and climate change separately, leading to fragmented and ineffective responses. There is a critical need for integrated governance structures that address these interconnected threats. **International cooperation** is essential to address the global nature of cyber threats and climate impacts. Initiatives such as the UNFCCC[38], Kyoto Protocol[39], and Paris Agreement[40] on climate change and international cyber norms aim to foster collaborative efforts, but more cohesive policies are needed. Australia and the United States cooperate on climate change with both countries engaging in bilateral climate change partnerships and working together in international settings like the Quadrilateral Security Dialogue[41], the Group of Twenty[42], and the Conference of Parties[43]. International climate change actions are primarily organized under the United Nations Framework Convention on Climate Change (UNFCCC). Under the UNFCCC, countries expanded climate change actions through the Kyoto Protocol in 1997 and the Paris Agreement in 2015. Under the 1987 Montreal Protocol, which was negotiated to ban substances harmful to the environment, the United Nations adopted the Kigali Amendment to ban potent greenhouse gases. Most United Nations members are party to these treaties. Australia is a party to all, but the United States is not a party to the Kyoto Protocol and withdrew from the Paris Agreement under the Trump Administration. The UNFCCC established the

---

[35] https://attack.mitre.org/groups/G0016/

[36] https://arpc.gov.au/resources/volt-typhoon-critical-infrastructure-an-ongoing-cyber-target/

[37] https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html#:~:text=Stuxnet%20is%20a%20powerful%20computer%20worm%20designed%20by,Stuxnet%20exploited%20multiple%20previously%20unknown%20Windows%20zero%20days

[38] https://unfccc.int/

[39] https://unfccc.int/kyoto_protocol

[40] https://www.dfat.gov.au/international-relations/themes/climate-change/international-cooperation-on-climate-change

[41] https://www.dfat.gov.au/international-relations/regional-architecture/quad

[42] https://www.oecd.org/en/about/oecd-and-g20.html

[43] https://www.unccd.int/convention/governance/cop

annual Conference of Parties (COP) which also serves as the meeting of the Parties to the Paris Agreement.

Data forecasting and prediction services

Climate change and cyber threats impact the accuracy and reliability of forecasting and prediction services, essential for public safety and economic stability. Not only will this disrupt global trade, but it will also affect critical industries such as energy and agriculture, and pose risks to financial system stability. In addition, cyber-attacks can disrupt critical climate monitoring services and directly cause environmental damage, hindering efforts to address climate change. This section looks at weather forecasting and prediction, data quality, and cyber risks to these systems.

Application and uses

Forecasting and prediction are key to the functioning of modern society and have implications for public health and safety, disaster prevention and recovery, food production and distribution, economy, trade and finance. For example, in terms of **public health and safety**, weather forecasts in high-income countries are more than five times as accurate as they were 40 years ago[44]. Studies show that having longer lead times on forecasts of severe winter weather reduces traffic accidents, saving lives but also having cascading effects on the economy due to reduced insurance costs and impact on sectors that could be impacted by the disruption to the transport system. Other uses of meteorological data in urban spaces include monitoring urban air quality, planning the capacity of combined storm and sewage systems, determining the location of new developments to avoid flood risk, and channelling of winds and/or urban heat islands[45].

In terms of **disaster prevention and recovery**, forecasting allows governments and organisations to alert individuals about extreme weather events ahead of time, allowing them time to adjust their actions and reduce exposure and/or vulnerability to such a weather event[46]. For example, the provision of advance warning of events such as wildfires, flooding and/or hurricanes provides the opportunity for individuals living or travelling in the area at risk, their families, the communities in which they live and the agencies with responsibilities for ensuring their safety, to make appropriate preparations to mitigate the adverse impacts from such events. Advance warning ahead of extreme events also benefits primary producers and those operating businesses, critical utilities and infrastructure (power, water, roads, etc.) directly by providing time to protect their assets and operations. Reducing potential damages and losses saves lives and assists insurance companies and governments by reducing the level of compensation and/or costs of funding relief and recovery operations. For example, it is estimated that forecasting the impact of flooding hurricanes in the U.S. has already improved by three times in the last four decades, reducing overall damage by 5%[47].

In terms of **food production and distribution**, the foresight of crop yield is fundamental to the agricultural industry to better mitigate and/or manage climate risks. Rain-fed crops are highly volatile and

---

[44] https://blogs.worldbank.org/en/impactevaluations/economic-benefits-weather-forecasting
[45] National Academy of Sciences (2012). Available at https://nap.nationalacademies.org/resource/13328/urban-meteorology-brief.pdf
[46] http://www.bom.gov.au/water/floods/document/National_Arrangements_V4.pdf
[47] https://blogs.worldbank.org/en/impactevaluations/economic-benefits-weather-forecasting

uncertain due to climate variability and change, impact costs and market prices[48]. Having advanced knowledge of the likely impact of the coming season's climate on crop yield and production is therefore critical for decisions across the supply chain.

Forecasting is also important for **economic trade**. Meteorological data is also essential to other sectors of the economy, such as the energy sector. For example, weather forecasting is critical to estimate peak energy demands (e.g., due to heat or cold waves) as well as forecast renewable energy supply. The increasing penetration of variable renewable generation in the grid will place even greater importance on weather forecasting to ensure the reliability of the energy supply. Forecasting whether key transport routes might be disrupted by extreme events is critical to minimise supply chain disruptions. Weather forecasting might also be critical to trade. For example, a study found that losses from market trade in Ghana could be reduced by 50% if extreme weather is anticipated[49].

Data quality

The lack of availability and/or accessibility of data for forecasting and predicting weather events at the local level could have a profound impact on a range of sectors and activities such as agricultural productivity and urban resilience, which could exacerbate social and economic inequalities. Local data should be used because individual localities are composed of a unique set of geographic, economic and socio-demographic characteristics, which impact the likelihood and severity of weather event impacts.

Under a changing climate, forecasting and predicting models that heavily rely on historic weather-related data are becoming less reliable, which may harm economic activity, public health and safety as well as the capacity of governments and communities to prepare for extreme climate events. This is because the conventional approach to risk assessment is based on a retrospective survey of historic hazards and impacts. As extreme events become more severe, more frequent, and/or more correlated, the true costs of climate-related damages tend to be underestimated. Human and capital investment is therefore needed for continuous improvement of forecasting tools for predicting the severity and frequency of weather hazards and the human and economic losses[50]. There is a large and growing need for high-quality climate information that improves climate-sensitive decisions across sectors and contributes to mitigation and adaptation goals. However, there are also concerns that climate science tends to produce outputs that are not user-friendly and/or that end-users may lack the technical capacity to interpret such outputs. It is therefore recommended that the provision of climate information is demand- or user-driven, meeting users' context-specific needs and their technical capacity. The goal might be to improve climate-sensitive decisions by making climate information 'useful, useable and used'[51].

Investing in data availability, quality and transparency as well as in human capacity might be a good avenue to improve climate forecasting and the useability of such data. For example, suggestions to improve tools available for data forecasting might include the creation of a data inventory, including the release of data that could be used to develop and test weather-hazard models. Governments hold a wealth of economic loss information from weather hazards, including data on financial damages at the property level. Subject to privacy considerations, making such data more easily accessible to research,

---

[48] Potgieter, A. B., Schepen, A., Brider, J., & Hammer, G. L. (2022). Lead time and skill of Australian wheat yield forecasts based on ENSO-analogue or GCM-derived seasonal climate forecasts – A comparative analysis. Agricultural and Forest Meteorology, 324, 109116. https://doi.org/https://doi.org/10.1016/j.agrformet.2022.109116
[49] https://blogs.worldbank.org/en/impactevaluations/economic-benefits-weather-forecasting
[50] George S (2023) A higher standard for climate risk modeling? WTW RESEARCH NETWORK NEWSLETTER. Available at https://www.wtwco.com/en-au/insights/2023/11/a-higher-standard-for-climate-risk-modeling
[51] Findlater, K., Webber, S., Kandlikar, M. et al. Climate services promise better decisions but mainly focus on better data. Nat. Clim. Chang. 11, 731–737 (2021). https://doi.org/10.1038/s41558-021-01125-3

non-profit, and private-sector modelling communities could help improve current data models. The upskilling of the modelling community is also critical for the improvement of climate forecasting[52].

Cyber risks

Cyber-attacks on Climate Monitoring organizations such as the National Oceanic and Atmospheric Administration (NOAA) can disrupt critical climate monitoring and forecasting services[1]. In 2014, NOAA was the target of a cyber-attack that compromised its weather and satellite systems. The attack temporarily disrupted the agency's ability to provide accurate weather forecasts and climate data, which are crucial for monitoring environmental changes and preparing for natural disasters. Another significant example is the 2017 WannaCry ransomware attack, which affected various critical infrastructure sectors worldwide, including some meteorological services. Such attacks can delay the dissemination of vital climate information, affecting everything from disaster response to long-term climate research. These disruptions can have cascading effects, hindering scientific research, delaying climate action, and compromising the reliability of data used to track global climate patterns.

Resilience and mitigation

Response strategies to build system resilience and/or mitigate climate and/or cyber threats tend to be well developed within sectors, but not yet between sectors. Addressing the nexus between climate change and cybersecurity requires coordinated efforts across policy, technology, and business practices. Cyber-attacks on critical infrastructure and climate-induced instability pose significant national security threats. This section explores current approaches to resilience and mitigation that can be explored on a global level.

Cyberattacks, natural disasters and disruptions to global supply chains directly impact the functioning of our critical infrastructure and are anticipated to increase significantly in scale and complexity over the coming decades. Countries such as the UK[53] and Japan[54] have national frameworks, with critical infrastructure protection and resilience policies generally driven by a singular hazard focus, such as climate change. Canada[55] requires sector-related information sharing to promote communication and hazard identification, but this is also focussed only on the impact of climate on physical disturbances.

Some countries have already recognised and begun to address the need for a multi-hazard focus. The USA[56], Switzerland[57], France[58] and Germany[59] have developed policies based on an all-hazards approach that provides holistic management and response to critical infrastructure threats and hazards. Even countries not advanced in the protection and resilience of their critical infrastructure acknowledge the

---

[52] George S (2023) A higher standard for climate risk modeling? WTW RESEARCH NETWORK NEWSLETTER. Available at https://www.wtwco.com/en-au/insights/2023/11/a-higher-standard-for-climate-risk-modeling

[53] https://www.npsa.gov.uk/critical-national-infrastructure-0

[54] https://www.nisc.go.jp/eng/pdf/cip_policy_2024_eng.pdf

[55] https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

[56] https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

[57] https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Focal-Report-1-CIP.pdf

[58] https://eur-lex.europa.eu/EN/legal-content/summary/european-programme-for-critical-infrastructure-protection.html

[59] https://www.openkritis.de/it-sicherheitsgesetz/kritis-dachgesetz-sicherheitsgesetz-3-0.html

importance of information sharing for system resilience to address the megatrends of climate change, digitisation, cyberattacks and rising geopolitical tensions. Although critical infrastructure policy frameworks are yet to be developed in the Oceanic region, countries such as New Zealand[60] have identified threats to cybersecurity, climate change and the criticality of data storage and processing infrastructure.

Strengthening collaboration and information sharing between stakeholders in all levels of government (local, national and international) as well as the public and private sectors and civil society is critical to identify shared responsibilities as well as develop and implement effective risk management practices to safeguard critical infrastructure. Collaboration is key to developing comprehensive climate and cybersecurity governance models to improve resilience and response capabilities, leading to more robust security practices and quicker responses to cyber incidents. For example, regional cooperation and initiatives can facilitate targeted strategies and resource sharing as well as address specific geopolitical challenges posed by climate change and cyber threats. Similarly, strengthening cross-sector collaboration within the private sector would assist businesses to incorporate climate change risks into cybersecurity strategies and help build more resilient infrastructures capable of withstanding both cyber and climate threats. Such cross-sector collaboration would be key in several stages including risk assessment and planning, resilient design and infrastructure, integrated incident response plans, as well as training and awareness activities.

Data and information exchange among stakeholders helps to enhance situational awareness and coordinated responses to threats. For example, the Climate Prediction Center (CPC) and National Centers for Environmental Information (NCEI) which operate within the National Oceanic and Atmospheric Administration (NOAA) share climate data and forecasts with stakeholders, helping to coordinate responses to climate-related threats and integrate this information into broader risk management frameworks[61]. Strengthening public-private partnerships may also help governments leverage innovative technologies and practices to improve the security and sustainability of critical infrastructure to enhance resilience against climate and cyber threats. Engaging communities in the decision-making process can also lead to more effective and inclusive solutions and ensure that strategies developed address the community's specific needs and vulnerabilities [62]. This is because the extent of impacts and capacity to respond to both climate change and cyber threats to critical infrastructure would be dependent on regions' socio-demographics and geographical characteristics. Communities characterised by resource restrictions, inequity, poverty and conflict are more vulnerable. Collaboration and data sharing would also help develop response strategies that consider the interdependencies of critical infrastructure sectors, which are largely lacking. To reduce the vulnerability to climate change and cyber-attacks it is critical that risk management approaches focus on integrated approaches that consider the various types of hazards and threats, how events compound and cascade as well as cross-sectoral and cross-national interdependencies.

Integrated policy frameworks that combine climate resilience and cybersecurity measures as well as evolve with emerging threats and changing environmental conditions can also help build system resilience. This might include harmonizing national security strategies with environmental policies to create a cohesive response to these dual threats, integrating climate resilience into economic and urban planning, developing regulations and strategies that encourage businesses to invest in climate resilience and allowing for timely and effective responses to new challenges. For example, it could include exploring the effectiveness of providing financial incentives for businesses to invest in climate adaptation and

---

[60] https://consultation.dpmc.govt.nz/national-security-group/critical-infrastucture-phase-1-public-consultation/user_uploads/discussion-document--strengthening-the-resilience-of-nzs-ci-system.pdf
[61] https://www.noaa.gov/
[62] https://www.undp.org/tag/communities-and-local-development

cybersecurity measures such as tax breaks, grants, and low-interest loans and/or establishing minimum security and resilience requirements for critical infrastructure projects receiving federal funding, ensuring compliance through robust accountability mechanisms. The development of **comprehensive risk assessment** frameworks that account for both climate and cyber threats would support organisations in developing and implementing their strategic planning to enhance resilience.

Developing and implementing cohesive **legal frameworks** that integrate cybersecurity and environmental governance is also critical for effectively dealing with this dual threat. Current national and international legal frameworks often treat cyber threats and climate impacts in isolation, lacking a unified approach to address the complex challenges posed by their intersection. For instance, cybersecurity regulations focus primarily on protecting data and IT systems, while environmental laws aim to mitigate pollution and manage natural resources. This separation can lead to gaps in addressing the interconnected risks where cyber incidents cause environmental damage or climate events exacerbate cybersecurity vulnerabilities. For example, the European Union's General Data Protection Regulation (GDPR), primarily focused on data protection, works in tandem with the Network and Information Security (NIS) Directive, which aims to improve the cybersecurity of critical infrastructure. This dual approach helps ensure that personal data protection and cybersecurity measures are aligned, creating a more resilient digital environment[63]. However, these directives do not address climate risks. On the other hand, the European Cyber Resilience Act (CRA)[64] establishes cybersecurity requirements for products with digital elements throughout their lifecycle. While focused on cybersecurity, the CRA's framework can also address climate resilience by protecting critical digital infrastructure from both cyber threats and environmental impacts. Integrating cybersecurity with environmental considerations safeguards essential systems, promoting a holistic strategy that aligns infrastructure protection with climate mitigation and adaptation efforts. The CRA serves as a model for evolving international agreements to tackle interconnected cybersecurity and environmental challenges, ensuring nations are better prepared to handle dual threats. Strengthening international agreements to include provisions for cybersecurity in climate policies can help nations prepare for and respond to interconnected threats.

To date, several approaches have been used to **develop resilience strategies within sectors**, including both reactive and preventive strategies. This might include a risk-based approach to identify and prioritize critical assets and systems based on their vulnerability to both cyber threats and climate impacts, which includes considering the likelihood, potential consequences, and cascading effects of disruptions[65]. Other strategies might include establishing clearly defined severity thresholds that trigger specific response protocols to ensure responses are timely and effective during incidents. Preventive strategies to address cybersecurity threats might, for example, include the implementation of advanced security protocols and continuous monitoring to defend against potential cyber threats. Other examples include incorporating redundancy, analogue controls, manual overrides where necessary and/or channel investments towards novel technologies and renewable energy sources to enhance overall system resilience. Investing and diversifying renewable energy can help improve the resilience of the energy system as the diverse characteristics of renewable energy sources make them vulnerable to different kinds of extreme weather events or disasters, with its distributed generation capacity also helping dilute impact[66]. True investment in resilience and mitigation would see both preventive and reactive risk management responses to assess and manage climate-related risks across the systemic value chain. In the aftermath of Hurricane Sandy in 2012, New York City undertook significant infrastructure investments

---

[63] https://gdpr-info.eu/

[64] https://www.european-cyber-resilience-act.com/

[65] https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

[66] Wang C, Ju P, Wu F, Pan X and Wang Z (2022) A systematic review on power system resilience from the perspective of generation, network, and load. Renewable and Sustainable Energy Reviews 167, 112567. DOI: https://doi.org/10.1016/j.rser.2022.112567.

to enhance resilience against future extreme weather events. This included the construction of the East Side Coastal Resiliency Project[67], a $1.45 billion initiative aimed at protecting vulnerable neighbourhoods from flooding and sea-level rise. Additionally, NYC Health + Hospitals implemented robust cybersecurity measures to safeguard its digital infrastructure, ensuring continued healthcare services during emergencies. But greater focus is still needed to invest in infrastructure design and upgrading with built-in resilience to withstand the simultaneous threat of both cyber-attacks and climate-induced events.

Strategies focused on **supporting communities** also have an important role to play in building community resilience and preparedness. For example, public awareness campaigns can help educate communities about the risks associated with climate change and cyber threats, and the importance of preparedness and resilience. Training and resources for local communities can also help enhance their capacity to respond to and recover from climate-related events and cyber-attacks. This includes first aid training, emergency response drills, and cybersecurity best practices. Enhancing social safety nets to support vulnerable populations during crises is also critical. Examples include financial assistance, access to healthcare, and housing support for displaced communities. Investing in capacity building for institutions responsible for cybersecurity and climate resilience can also enhance the institutions' ability to anticipate, prepare for, and respond to complex threats.

Key takeaways

Increasing risk complexity and the need for new, more sophisticated mitigation responses are driving uncertainty - impacting action and investment decisions across government and industry. There is also an emerging loss of community confidence regarding the ability of government and businesses to ensure essential services continue during and after hazard events. Climate change and cyber-security threats to critical infrastructure are likely to increase. The protection of critical infrastructure against the dual threats of climate change and cyber-attacks is a multifaceted challenge with profound and far-reaching implications for society. While a range of strategies are being developed or underway to ensure the security and resilience of critical infrastructure systems, much still needs to be done.

Cross-sectoral, national and international collaboration is key to continue developing knowledge and strategies to improve our understanding of such risks, reduce the vulnerability of critical infrastructure and protect the functioning of society. Systemic risk governance is essential to develop and implement comprehensive, inclusive and integrated policy strategies that strengthen the resilience of both physical infrastructure and communities and enhance community preparedness. A coordinated effort nationally and internationally across various sectors and governance levels that spans policy, technology innovation, and business practice is key to implementing effective responses.

---

[67] https://www.nyc.gov/assets/escr/downloads/pdf/ESCR-Final-Scope-of-Work_040519.pdf

Scenario Mapping

To facilitate the identification of knowledge gaps, recommended investments, and other actions needed to manage risks at the intersection of cyberphysical systems and climate change, attendees will take part in a series of small-group activities throughout the course of the workshop. Attendees will explore one of three attack scenarios. Attendees will be assigned to act in certain roles for each scenario; as possible, assignments will be based on participant affiliations and expertise. Background context for each scenario has been provided in the read-ahead briefing packet. Specific scenario briefings will be distributed to each breakout group on the second day of the workshop, Tuesday, July 30. These briefings will include details about a hypothetical attack taking place in an imaginary 2030 with various short-term climate, technological, geopolitical, and economic developments. The briefings will also define player roles in terms of the stakeholder organization they represent, their responsibilities/authority (i.e., basic guidance on actions within the role's ability to execute or influence), and their motivations (i.e., basic guidance on objectives the role wants to accomplish).

This is not a traditional tabletop exercise. Rather than playing through one instance of how a scenario could evolve, participants will collaboratively develop a "scenario map" by alternately considering actions that their and other roles might take, as well as the outcomes or impacts of those decisions. This design will allow us to map out a larger space of plausible outcomes to the scenario, only some of which may be positive or desirable. After organizing the scenario map as a sequence of actions and outcomes, participants will rate each element in terms of its likelihood (i.e., contingent upon reaching a previous branch in the map, how likely this outcome would occur or how likely is it that an action would be taken?) and its desirability (i.e., how good or bad is this outcome?).

Participant input will guide the design of related scenarios to be explored on the last day of the workshop, Thursday, August 1. These scenarios will envision what the year 2050 could look like as a long-term outcome of decisions made in one or more branches of the 2030 scenario map. Activities on this day will include another scenario mapping elicitation and a hindcasting exercise asking participants questions about how the attack could have been prevented, when action would have been needed, what data could have revealed the risk(s), and what type of investments could have yielded those data.

Restaurant Recommendations

Location	Cuisine	Address	Distance
Alero Restaurant	Mexican	1629 Connecticut Ave. NW	~5 min. walk
Banana Leaves Asian Restaurant & Sushi Bar	Asian	2020 Florida Ave. NW	~1 min. walk
Bibibop Asian Grill	Asian	1516 Connecticut Ave. NW	~8 min. walk
Café Integral	Coffee	1900 Connecticut Ave. NW	~5 min. walk
Dolcezza Gelato & Coffee	Coffee	1704 Connecticut Ave. NW	~4 min. walk
Emissary	Coffee	1726 20th St. NW	~3 min. walk
Firehook Bakery	Coffee	1909 Q St. NW	~7 min. walk
Hoja Taqueria	Mexican	1900 Connecticut Ave. NW	~5 min. walk
Kramerbooks & Afterwords Café	American	1517 Connecticut Ave. NW	~7min. walk
La Tomate	Italian	1701 Connecticut Ave. NW	~3 min. walk
Lauriol Plaza	Tex-Mex	1835 18th St. NW	~5 min. walk
Le Pain Quotidien	Bakery	2000 P St. NW	~9 min. walk
Mi Casa	Mexican	1647 20th St. NW	~5 min. walk
Panera Bread	Takeout only	1528-5 Connecticut Ave. NW	~7 min. walk
Pizzeria Paradiso	Pizza	2003 P St. NW	~9 min. walk
Rakuya	Japanese	1900 Q St. NW	~7 min. walk
Sette Osteria	Italian	1666 Connecticut Ave. NW	~4 min. walk
Starbucks	Coffee	1501 Connecticut Ave. NW	~7 min. walk
Sweetgreen	Salads	1512 Connecticut Ave. NW	~8 min. walk
Taïm Mediterranean Kitchen	Mediterranean	1514 Connecticut Ave. NW	~8 min. walk
Tatiana Pizza	Pizza	1730 Connecticut Ave. NW	~3 min. walk
Teaism Dupont Circle	Asian	2009 R St. NW	~5 min. walk
Thai Chef Street Food	Thai	1712 Connecticut Ave. NW	~4 min. walk
Thaiphoon	Thai	2011 S St. NW	~2 min. walk
Zeleno	Café	1605 Connecticut Ave. NW	~6 min. walk
Zorba's Café	Greek	1612 20th St. NW	~6 min. walk

Notes