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

Summary of Speaker Presentations

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

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

NATO OTAN

This workshop is supported by: The NATO Science for Peace and Security Programme

U.S. Department of Homeland Security

Science & Technology

Summary of all Speaker Presentations

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

NATO Advanced Research Workshop | July 29–August 1, 2024

Abbreviations

Abbreviation	Definition
AI	Artificial intelligence
cm	centimeter
CO2	Carbon dioxide
CPSICC	Cyber-Physical-Social Infrastructure Climate Change (CPSICC) Nexus Workshop
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DHS	Department of Homeland Security
EEA	European Environment Agency
EV	Electric vehicle
IPCC	Intergovernmental Panel on Climate Change
km	kilometer
NATO	North Atlantic Treaty Organization
NNSA	National Nuclear Security Administration
qubit	Quantum bit
S&T	Science and Technology
Sandia	Sandia National Laboratories
SIIP	Socially Integrated Infrastructure Planning

Opening Session

Welcome from Purdue University

Matthew Huber, Purdue University

Matthew Huber provided a welcome from the workshop organizers on behalf of Purdue University. He noted that the workshop aimed to explore the complexity of interconnected systems, using examples such as heat waves and pandemics to illustrate how different components — social, physical and infrastructural — interact within a risk framework. He emphasized the dual potential for these interactions to either enhance resilience or exacerbate risks, depending on responses and system characteristics, such as exposure, hazard, vulnerability and response. Huber noted the workshop focus was to advance our understanding of these dynamics by identifying gaps in knowledge and planning for comprehensive data collection. He noted workshop outcomes were to include a summary report, a short white paper and

potentially a book or journal special issue. Huber also shared that a dedicated website was created to disseminate the workshop results.

Welcome from CSIRO

Marthie Grobler, *CSIRO*

Marthie Grobler extended a welcome from CSIRO, Australia's national science agency. Grobler stressed the need to address the escalating complexity of interconnected hazards impacting critical infrastructure, highlighting the growing number of threats and their spillover effects. Her presentation underscored the need for sectors to collaborate and share information to manage these risks effectively. She focused on compound hazards that arise from interdependencies among independent sectors, leading to cascading impacts that have implications where critical infrastructures converge.

Grobler then shared that CSIRO's cyber research focuses on critical infrastructure and critical technologies, looking at highly dependent critical infrastructure within the energy and communications sectors, and leveraging advancements in AI, quantum technology and digital twins to address cybersecurity issues. She explained their research aims to improve critical infrastructure resilience by understanding and adapting to security challenges with a human-centric focus. Grobler's presentation emphasized the importance of integrating climate and cybersecurity considerations into both digital and physical infrastructure. She advocated for a comprehensive understanding of global interdependencies and risks, identifying knowledge gaps and fostering international collaboration for enhanced capability and transparency. Grobler noted that a workshop goal was to improve global resilience by combining diverse perspectives and expertise.

Welcome from Sandia National Laboratories

Rossitza Homan, *Sandia National Laboratories*

Rossitza Homan provided an overview of Sandia National Laboratories, a federally funded research and development center under the National Nuclear Security Administration. As Homan shared, Sandia's core mission is to design, test, and maintain the U.S. nuclear stockpile, ensuring national security through nuclear deterrence. She highlighted how this expertise translates into broader scientific and technological applications, enhancing resilience in critical systems worldwide. For example, Sandia's diverse capabilities have resulted in technologies such as clean rooms for chip production to withstand nuclear environments, portable biological detectors like the mobile SpinDX device, a hydrogen fuel cell-powered green ferry, unmanned aerial vehicles and robots used by warfighters, and a significant renewable energy portfolio, including efficient wind turbine blades. She reiterated that these innovations contribute to both national security and environmental sustainability.

Homan then emphasized the complex interactions within and across the cyber-physical, social, and natural environment nexus. She shared that both the NNSA administrator and Sandia consider climate change as an existential threat, paralleling nuclear risks. Homan explained that one focus of the workshop was to identify research and partnership gaps to foster impactful collaborations. Homan highlighted other presentations from Sandia representatives set to occur during the workshop that would cover different aspects of the cyber-physical-social and natural environment nexus including security, deterrence, and defense; climate security and integrated deterrence; resilience of health, food and agriculture systems; analytical gaming; and three worldviews of water as a complex system.

Welcome from NATO

James Appathurai, *NATO Innovation, Hybrid and Cyber*

James Appathurai welcomed participants on behalf of NATO through his pre-recorded remarks. Appathurai outlined the collaborative efforts between NATO and the U.S. Department of Homeland Security in addressing evolving security challenges. He highlighted the recent NATO summit in Washington, D.C., which emphasized NATO's commitment to supporting Ukraine, strengthening defense and deterrence and enhancing partnerships.

He shared that NATO is focused on the energy transition, security, climate change and undersea infrastructure, with resilience as a central theme. He talked about how the alliance is adapting to the impacts of climate change on security, driven by the Russian invasion of Ukraine and international climate agreements, such as the Paris Agreement. Appathurai described these adaptation measures, which includes managing threats, such as sabotage of energy infrastructure and increased cyber risks due to the interconnected nature of diverse energy sources and AI-driven systems. To address hybrid threats, he reported that NATO is enhancing resilience in civilian and critical infrastructure, focusing on cyber protection. This work involves developing a cyber pledge aligned with European Union targets and improving the security of undersea infrastructure through shared sensor data.

Additionally, he shared NATO's commitment to mitigating climate change impacts by adapting forces and infrastructure, targeting net-zero emissions by 2050 with a 46% reduction by 2030, and investing in new technologies through an innovation fund to support these goals.

Welcome from the U.S. Department of Homeland Security Science & Technology Directorate

Julie Brewer, *U.S. DHS S&T*

Julie Brewer also extended a welcome to workshop participants through pre-recorded remarks. Brewer outlined the mission and focus areas of the Department of Homeland Security, emphasizing its commitment to safeguarding against both natural and man-made threats. Central to this mission, she outlined, is the Science and Technology Directorate, which plays a crucial role in research and development aimed at solving operational problems and providing support and guidance to first responders. This directorate employs evidence-based and technical perspectives to enhance its effectiveness.

Brewer then identified gaps and prioritization of resources as key to tackling the complex challenges facing homeland security. The S&T Directorate focuses on addressing known risks while acknowledging the presence of numerous unknowns due to global changes. She explained that this work involves developing and deploying dual-use technologies that serve both homeland security objectives and the needs of first responders.

By addressing these priorities, Brewer suggested the DHS can bolster national safety and security through innovative solutions and strategic resource management. She noted that this approach underscores the importance of adapting to evolving threats and leveraging advanced technologies to improve resilience and response capabilities.

Setting the scene: Laying out the landscape of the CPSICC NEXUS through 2050

David Johnson, *Purdue University*

David Johnson introduced the workshop participants to the small group activities scheduled for Wednesday and Thursday, which were designed to explore various scenarios and knowledge gaps related to attacks on infrastructure exacerbated by climate change. He explained how the activities would employ branching scenarios to simulate a range of potential attacks and identify diverse responses.

Johnson then gave a brief summary of the three scenarios: Arctic Shipping Lanes, Opportunistic Power Grid Outages and Solar Radiation Modification. For the Arctic Shipping Lanes scenario, participants would address geopolitical tensions, develop technologies and strategies to counter vulnerabilities, and explore international cooperation to mitigate cybersecurity threats. For the Opportunistic Power Grid Outages, participants would focus on creating contingency plans for smart grid infrastructure, assessing impacts from climate events and prioritizing national responses during extreme weather combined with cyber incidents. In the third scenario,

Solar Radiation Modification, participants would discuss international governance for regulating research, development and deployment of solar radiation modification technologies; protecting these technologies from adversarial interference; and managing transboundary impacts.

Johnson shared that each group would comprise a mix of subject matter experts and non-SMEs. Each participant would assume a role within their group and brainstorm and develop strategies specific to their role. Johnson articulated that this role-based approach was designed to foster comprehensive discussions and innovative solutions for each scenario.

He advised participants to review the briefing materials before the sessions to ensure informed and effective participation. The workshop organizers structured the activities to capture a broad spectrum of potential impacts and responses, highlighting the importance of addressing multiple dimensions of infrastructure vulnerabilities and climate-induced challenges.

Plenary talk on emerging security challenges

NATO strategic line of effort

Eyüp Turmuş, *NATO SPS Programme*

Eyüp Turmuş outlined NATO's initiatives to address climate change and security, emphasizing their long-standing focus on these issues. Since 1969, NATO has been engaged in understanding the impacts of climate change on security, alongside challenges such as pollution and health risks. The 2021 NATO summit reaffirmed the alliance's commitment to integrating climate considerations into security strategies.

Central to NATO's efforts, Turmuş explained, is the Science for Peace and Security program, which fosters collaboration between NATO and partner countries through civil science and innovation. The SPS program is guided by strategic concepts and provides grants to organizations, universities and agencies. He noted that the SPS program operates on a structured call-for-proposals process approximately three times a year, with submissions peer-reviewed by independent experts.

The SPS program supports various mechanisms for cooperation, including research and development projects typically spanning two to three years, and funding for equipment, travel and stipends. He noted the program also organizes events, such as workshops and training courses, including accommodations. Each project must involve at least one NATO member and one partner country.

Turmuş highlighted that NATO emphasizes consensus in decision-making and promotes partnerships and interoperability through shared standards and practical training exercises. The SPS program facilitates the integration of diverse stakeholders, including industry and startups, to address security challenges holistically. By engaging with private industry and supporting new technologies, he conveyed that NATO aims to ensure comprehensive, multi-faceted approaches to contemporary security issues and climate-related threats.

Plenary talk on emerging security challenges

DHS strategic line of effort

David Alexander, *U.S. DHS S&T*

David Alexander highlighted emerging areas in strategic foresighting and earth sciences research, emphasizing the need for a comprehensive approach to address evolving global challenges. Alexander started by noting the need for holistic homeland security, meaning that security should extend beyond the Department of Homeland Security to include public and private sectors, and first responders. He highlighted world interdependence as a critical security issue — as global interconnectedness increases, it creates more complex, evolving threats and challenges that defy traditional boundaries and frameworks. He then illuminated the multifaceted nature of the challenges at the intersection of climate and security. This complex nexus involves not just national but global concerns, necessitating broader collaboration. Not only is this nexus complex, but as he noted**,** this nexus has expanded to now include social and ecological systems, reflecting the interconnected nature of modern infrastructure and environmental systems.

Alexander explained how known risks are evolving in unpredictable ways. Scientific advancements are reshaping infrastructure systems, introducing both known and unknown threats. He discussed specifically how the ongoing energy transition poses security risks. For example, technological innovations like lithium-ion batteries pose new safety and security risks that must be managed without stifling progress. Alexander noted the cross-cutting nature of these challenges. He cited climate change impacts, including migration, displacement and social instability, all as challenges that could affect infrastructure systems.

Alexander then explored the research gaps at this nexus. He espoused the need for better questions and interdisciplinary approaches to address the multidimensional nature of these issues with key areas including nature-based solutions, geoengineering and digital solutions. He also called for a systems perspective to risk assessment as crucial for understanding and mitigating cascading failures and vulnerabilities, balancing resilience and functionality. Alexander argued that effective policy and research must integrate AI with social sciences, address technological gaps and prioritize stakeholder inclusion to anticipate and manage future risks. At the same time, he pointed out that the lines between public safety and security are becoming increasingly blurred in the context of climate change. Lastly, Alexander touched on the fact that much of our infrastructure systems and societal structures were built for yesterday's climate and society and not the evolving risks, hazards and risk landscape of today.

Overall, Alexander called for a proactive, systems-based approach to research and policy development, incorporating diverse perspectives to better address the complexities of modern threats and vulnerabilities.

Closing remarks

Matthew Huber, Marthie Grobler and Rossitza Homan

In closing remarks, Matthew Huber emphasized the necessity of innovative thinking to prevent disasters by investing in clean energy and resilient infrastructure. He warned against the risks of a "move quickly and break things" approach in the context of the nexus of technology, infrastructure and adversarial threats. He explained the importance of thoroughly understanding and addressing the vulnerabilities associated with new technologies and policies, especially in areas like the Internet of Things, to avoid adverse impacts on people.

Marthie Grobler underscored the importance of challenging established thought patterns. She highlighted that maintaining the same mindset will lead to predictable outcomes, urging a shift in approach to achieve different and potentially better results.

Rossitza Homan discussed the importance of a systems perspective in understanding complex behaviors and interactions relevant to national and global security. She noted Sandia's work with the DHS National Infrastructure Simulation and Analysis program to model critical systems and study potential future pandemics. Homan stressed the need for actionable research that goes beyond scientific advancements to address real-world impacts on human lives and infrastructure, ensuring that research translates into meaningful change.

Day Two

Introduction/Initial Exhortation

Matthew Huber, *Purdue University*

Matthew Huber started the second day of the workshop with a presentation on the critical issue of heat stress and its escalating impact due to global warming. Huber highlighted the urgent need to understand and mitigate the effects of increasing temperatures on human health, labor productivity and societal structures. He focused on heat stress, which has profound implications for various subsystems including health, labor, infrastructure, and energy demands.

Historically, according to Huber, heat stress research began with Haldane’s 1905 metrics, particularly the wet-bulb temperature, which measures the maximum temperature at which sweat can effectively cool the body. He explained that modern research reaffirms that high wet-bulb temperatures can lead to severe health consequences and reduced labor capacity, with significant societal implications. He noted that even modest increases in global temperature can shift current temperature thresholds to levels where prolonged exposure becomes deadly.

Huber then presented on recent studies that reveal that as global temperatures rise, areas like India, Pakistan and West Africa will experience dangerously high wet-bulb temperatures more frequently. He explained that these conditions threaten outdoor laborers and can lead to substantial economic losses and increased poverty, particularly in developing countries. Huber emphasized that while higher-income regions may have more resources to adapt, the Global South will face severe challenges, exacerbating global inequalities.

Huber also critiqued the reliance on traditional climate change mitigation strategies, such as irrigation, which, while reducing maximum temperatures, can worsen humidity levels, thereby diminishing the effectiveness of human perspiration. He illustrated how the integration of wet-bulb globe temperature metrics into climate models helps quantify these impacts on labor productivity and the global economy. In conclusion, Huber called for comprehensive adaptation strategies and international support

to address these disparities. He cautioned that failure to act could lead to increased mortality, economic instability and potentially massive migration pressures, highlighting the need for urgent, coordinated global responses.

Future climate change and insights into the implications for energy, communities, and economies

Richard Matear, *CSIRO*

Richard Matear provided an update on the state of carbon dioxide emissions and their impact on future climate scenarios, emphasizing key findings from recent assessments and projections. Matear shared how CO_2 emissions have been tracked through the Intergovernmental Panel on Climate Change's 5th and 6th assessments, which utilize Shared Socioeconomic Pathways to model different emission scenarios. While the highest emissions scenarios are no longer being tracked, he shared that current emission reduction efforts are insufficient to prevent a 2°C increase in global temperatures by the end of the century. He explained the lowest emissions scenario involves unproven technologies that could include climate intervention measures, though these come with new risks, such as aerosols affecting weather patterns.

Matear noted that future climate scenarios are based on Coupled Model Intercomparison Project climate projections, which examine how extreme weather events and variability change with global warming. Presently, he noted, the global mean temperature has risen by 1.3°C, with this warming trend accelerating. He pointed to extreme weather events, including droughts, fires and floods, becoming more common, particularly in regions like Australia, where high variability already exists. He demonstrated the economic costs of these events are substantial, impacting both global and local economies.

He then discussed how climate modeling is evolving to address these issues, transitioning from large global models to finer-resolution regional models to better capture weather events. Despite improvements, he pointed out that models still struggle with critical processes like ice sheet melting and tipping points. He shared regional models, with resolutions from 100 kilometer to 10 km, provide more accurate simulations of weather phenomena but cannot perfectly replicate real-world conditions.

Matear noted that projected changes in hazards include increased frequency and intensity of heatwaves, extreme fires, sea level rise and extreme rainfall. He conveyed that sea level rise, ranging from 28 centimeters to 101 cm, will exacerbate flooding risks, leading to more frequent and severe coastal inundation. Matear also shared that extreme rainfall, coupled with drier conditions, will result in more runoff and flooding. He noted the rate of global warming is accelerating, partly due to reduced aerosol emissions from coal burning, which previously had a cooling effect.

In summary, Matear shared that climate change is progressing rapidly, with events becoming more frequent and severe. He pointed to human actions, particularly greenhouse gas emissions, as the drivers of these changes. Matear summarized the adaptation strategies and technologies under consideration, such as climate intervention, as presenting both opportunities and uncertainties and thus necessitating ongoing evaluation and adaptation.

The first European Climate Risk Assessment: How to support policy prioritization in a complex risk and political context

Hans-Martin Füssel, *European Environment Agency*

Hans-Martin Füssel presented on the first European climate change risk assessment, coordinated from 2022 to early 2023, with the aim to provide scientifically valid and politically relevant information under tight constraints. Füssel explained this assessment, part of the European Union Green Deal, sought to identify adaptation-related policy priorities for the upcoming European Commission. He shared that the assessment focused on infrastructure, leveraging existing knowledge from IPCC reports and other climate impact modeling projects, and employed semi-qualitative methods due to time constraints. Füssel noted that the European Environment Agency, which is celebrating its 30th anniversary and plays a pivotal role in bridging knowledge and policy, aided in the assessment.

Key aspects of the assessment according to Füssel were understanding EU competencies, such as exclusive, shared, and supportive competences, that influence climate-sensitive sectors and policies. He noted the assessment was driven by the EU Green Deal and the new adaptation strategy announced in 2021, leading to the EEA's involvement in conducting the risk assessment.

Füssel shared that the assessment focused on major climate risks requiring European or transnational action, particularly complex climate risks, cascading risks and cross-sectoral impacts. Due to the short timeline, he noted that new quantitative modeling was not feasible; instead, the assessment relied on existing data and semi-qualitative methods. He also articulated that the assessment excluded national adaptation policies and security risks due to time and expertise limitations.

Füssel noted the assessment identified 36 major risks, grouped into five clusters: ecosystems, food, health, infrastructure, and economy and finance. He highlighted the urgency of action across all clusters, with heat stress identified as a major silent killer. Füssel shared the assessment's emphasis on the importance of non-climatic factors and the cascading impacts of climate risks, advocating for integrated policy responses.

Overall, Füssel asserted that the first European climate risk assessment successfully provided a comprehensive overview of climate risks and policy priorities, emphasizing the need for urgent action to mitigate significant environmental, economic, and social impacts. He noted the assessment has received strong uptake from EU institutions and stakeholders, reflecting its relevance and importance.

Compound and cascading climate hazards and their impacts on critical infrastructure systems

Amir AghaKouchak, *University of California Irvine*

Amir AghaKouchak presented on the complexities of coastal and fluvial flooding and highlighted the limitations of current flood risk assessment guidelines. AghaKouchak shared that coastal areas often experience multiple types of flooding — oceanic, fluvial and terrestrial — which interact in complex ways. He acknowledged that existing guidelines typically treat these hazards separately, leading to significant underestimation of flood risk. He gave as an example the combination of fluvial and ocean flooding in assessments reveals up to a 20% increase in failure probability compared to univariate models, and this risk further escalates with projected sea level rise.

AghaKouchak shared that his research in U.S. coastal environments indicates that current univariate methods inadequately address compound flood scenarios. He argued that the integration of multivariate approaches, which consider the interaction between different flood drivers, can provide a more accurate

risk assessment. For instance, he illustrated how estuaries in open landscapes like Alaska may migrate upstream with sea level rise, but in areas with constrained built environments, such as California, this migration is impossible, significantly affecting flood risk.

AghaKouchak advocated for linking statistical models to physical models to better bridge the gap between climate science and engineering. He clarified how this approach includes considering physical failure mechanisms, such as erosion and slope failure, which—results in a dramatic increase in failure probability even without extreme future scenarios.

He categorized compound events into four types: multivariate, spatially compound, temporally compounding/cascading and preconditioned compound. He shared that scientists have developed generalized models for multi-hazard scenarios and emphasized the need to incorporate observed increases in extreme weather events into infrastructure design. He clarified that by using process-informed non-stationary extreme value analysis, we can account for physical drivers like land use changes and climate scenarios, which suggests higher infrastructure loading requirements.

AghaKouchak argued adaptive design concepts are essential for updating flood defenses. He noted these frameworks should monitor changes, estimate their likelihood and incorporate equity considerations. He asserted that cascading hazards, such as drought leading to increased fire risk and subsequent debris flows, highlight gaps in existing risk models, which often fail to address the time dimension and spatial interactions of such events. Overall, AghaKouchak concluded there is a need for more robust models that account for the complex interactions of cascading and compound hazards across time and space.

Cybersecurity and climate change nexus: Applying risk-based approaches to ensure resilience and critical mission assurance of cyber-physical systems

Piret Pernik, ***NATO Cooperative CyberDefence Centre of Excellence***

Piret Pernik introduced herself as a researcher at NATO Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia, where her work focuses on the intersection of cyber security and climate impacts. Pernik outlined three key questions to be addressed in her talk: how climate impacts the cyber security sector, the sustainability of the cyber security/information communication technologies sector, and how to manage these risks.

She noted that cyber security has long envisioned catastrophic scenarios as possible but that the economic cost of cyber-attacks is still lower compared to climate-induced damages. She articulated that both cyber and environmental risks can act as risk multipliers, intensifying each other's impacts.

Pernik described how critical infrastructure, including military operations and essential services, heavily depends on information and operational technologies. She relayed that cyber-attacks can manipulate environmental data and spread disinformation, as seen with Russia and China's strategies. She pointed out that direct risks include physical harm to infrastructure, while indirect risks involve supply chain disruptions and relocation of critical infrastructure without adequate cyber security measures.

Pernik then focused on growing concerns related to the carbon footprint of the ICT sector, including data centers and AI. Although estimates vary, Pernik acknowledged that the sector's emissions will most likely continue to increase. She explained that AI's energy consumption is particularly uncertain but is expected to rise significantly. Conversely, Pernik expressed how new technologies could potentially reduce emissions through optimized power grid operations and energy management. She relayed that the cyber security sector often overlooks sustainability in procurement decisions, and there is a lack of

guidelines for adopting green technologies. She pointed out that policy agreements and strategies, such as the UN's draft digital compact and the EU Green Deal, acknowledge the need for sustainable digital technology, but specific integration of climate considerations into cyber security policies is missing.

To address these challenges, Pernik contended we need better data, transparency from AI companies, more comparative studies on the sustainability of cyber security infrastructure and specific guidance on integrating climate-related hazards into digital risk management. She communicated that cross-fertilization of risk management concepts can enhance resilience and business continuity across both types of risks. She also argued for the adoption of sustainable cyber security solutions and monitoring their effectiveness is crucial for a resilient future.

Extreme weather trends against datacenters and cryptocurrency functionality

Sunny Wescott, *U.S. DHS CISA*

Sunny Wescott presented on the multifaceted impacts of climate change on critical infrastructure sectors, focusing on data centers and energy systems. Wescott asserted that many infrastructures, including data centers, were constructed prior to the current climate realities, leading to vulnerabilities exposed by rising temperatures and extreme weather events. For instance, she cited high heat and precipitation as processes that can accelerate material degradation, impacting the reliability and efficiency of these facilities.

She pointed to global phenomena, such as simultaneous flooding events in Texas and Brazil, as illustrations for how extreme weather exacerbates competition for resources, leading to increased repair and rebuilding costs. Wescott explained how this competition is compounded by the fact that data centers, essential for modern digital operations, were not designed to withstand current climate extremes. As climate conditions worsen, she reasoned these facilities will face challenges related to cooling efficiency and structural integrity, necessitating significant resource allocation for maintenance and emergency responses.

Wescott further explored how these impacts are not isolated to one region but are part of a global trend. She pointed to data centers in major hubs like China, India, and Ireland that are also experiencing heightened risks due to extreme weather, affecting their operational capabilities and resource needs. She noted that the increasing demand for AI and data processing will amplify these pressures, stressing existing infrastructure and driving the need for innovative climate resilience strategies.

Wescott concluded that the interaction between climate change and critical infrastructure underscores the urgency for adaptive measures to mitigate risks, enhance resilience, and ensure sustainable operation in the face of escalating environmental challenges.

Risks and opportunities for cybersecurity posed by quantum technology

Marcin Niemiec, AGH University of Krakow

Marcin Niemiec discussed quantum technology and its significant influence on cybersecurity, both positive and negative. Niemiec remarked that quantum technology can produce innovative cybersecurity solutions that enhance security levels. However, he also acknowledged it poses considerable risks because quantum computers could potentially break current cryptographic methods. He advised that this dual nature of quantum technology makes it a critical topic in telecommunications and computer science. He

expressed gratitude for the invitation to the workshop, which provided a new perspective on integrating quantum technology with climate change considerations.

Niemiec began with an overview of quantum physics basics, focusing on quantum bits and their unique properties. He explained qubits can exist in a superposition of states, allowing for more complex information encoding than classical bits. He shared key quantum effects to include the measurement effect, the non-cloning theorem and quantum entanglement, all of which have significant implications for data protection and communication.

Niemiec then discussed quantum random number generators and quantum key distribution as opportunities for enhancing cybersecurity. He noted that quantum random number generators produce truly random numbers, essential for many aspects, e.g., cryptographic keys or simulations. He explained that quantum key distribution, combining symmetric cryptography with quantum channels, offers secure key exchange mechanisms that are resistant to eavesdropping.

However, Niemiec implored, quantum technology also presents risks, particularly the potential of quantum computers to break asymmetric cryptography. To address this, he pointed to the development of the field of post-quantum cryptography, which focuses on creating algorithms that can withstand quantum attacks. Niemiec mentioned the Post Quantum Cryptography Framework for Energy Aware Contexts or PQ-REACT project, which focuses on fast and smooth transition to post-quantum cryptography to do things like test the efficiency of such algorithms.

Niemiec also explored the application of post-quantum cryptography to climate change, emphasizing the need for robust cryptographic solutions to protect smart grids and other critical infrastructure from cyber threats. He concluded by acknowledging the challenges of implementing quantum cryptography, including issues of stability, scalability and infrastructure reliability.

Plenary Talk: Climate security and integrated deterrence

Rob Leland, Sandia National Laboratories

Rob Leland addressed the integration of climate security and deterrence within the broader framework of national and global security. Leland, along with co-authors, developed an analytical framework to link climate security risks with deterrence strategies, emphasizing the need to reduce adversaries' perceptions of the net benefits of aggression.

He defined climate security as encompassing political, physical, economic, and social stability in the face of climate change. He shared that integrated deterrence, as defined by the 2022 National Defense Strategy, involves leveraging all instruments of national power across domains and working with allies to deter adversary actions. This framework, he noted, aims to incorporate climate security into a deterrence construct, providing strategic value.

Leland shared that the team identified six key climate security risks areas: tensions over climate responses, energy transition risks, changing polar access, increased great power conflict, threats to human systems, and risks associated with climate intervention. The team based these risks a reason the National Intelligence Estimate, with the goal to highlight potential geopolitical tensions and the need for robust responses.

Drawing from historical literature and analysis, the team developed a deterrence model with four criteria for effectiveness: communication, credibility, capability and calculation. Leland explained that effective deterrence requires clear communication of counter-threats, credibility of those threats, demonstrated capability to execute them and the adversary's informed consideration of the consequences.

He elaborated on specific adversary actions to be deterred, such as rogue climate interventions and competition in the Arctic. He added that the framework maps necessary capabilities to support deterrence, including detection and attribution, cost and consequence modeling, and global governance structures.

Leland then presented the R&D required to support these capabilities, including in areas like high-resolution climate modeling, remote sensing, impact analysis and critical infrastructure risk assessment. He emphasized the need for international standards and systems engineering to integrate various components into an effective deterrence capability.

Overall, Leland underscored the complexity of integrating climate security into national defense strategies and the need for comprehensive, adaptive and collaborative approaches to address emerging threats in a changing climate.

Introduction to Smart Games and CPSICC Gameplay

David Johnson, *Purdue University*

David Johnson outlined a two-day exercise focused on risk elicitation and scenario mapping for 2030 and 2050. Johnson pointed participants to the scenario briefings available online, and shared gameplay logistics, including the use of real-time transcription for data collection, avoiding personally identifiable information, and rating outcomes via Google Sheets. He reminded attendees that participation was voluntary, and that the goal was to play a collaborative, informative game rather than to win.

Johnson emphasized active listening, respectful challenges, confidentiality, and collective goals as ground rules. He shared that the schedule was to conduct the 2030 scenario mapping on Wednesday morning, followed by lunch discussions and afternoon evaluations.

During lunch, he encouraged participants to discuss and reflect on their scenarios. In the afternoon, he shared that participants would rate the likelihood and impact of responses and outcomes, focusing on disagreements and research gaps. On Thursday, he clarified that participants would use the same scenarios but mapped for 2050 using 2030 outcomes. Johnson explained that participants would engage in hindcasting to identify preventative measures, necessary actions, and required data or technology.

Short Talks

Not breaking the bank: Where climate technology could maintain financial system stability

Nick Heavens, *Viridien*

Nick Heavens explored the need for creating climate scenarios to assist in reverse stress testing for financial institutions. The key issue Heavens addressed is the negotiation between regulators and banks regarding scenarios that might force banks to hold more capital or take costly measures. As he explained, banks prefer scenarios that avoid such outcomes.

Heavens focused on the financial system's instability, particularly concerning counterparties like insurers and sovereigns, including countries and U.S. states. A notable example he gave was the U.K. pension funds' crisis during Elizabeth Truss's tenure as Prime Minister, where proposed economic policies led to a loss of confidence and a drop in bond prices, causing significant financial strain. He used this situation to highlight how rapid negative changes in asset value or widespread loan defaults can destabilize financial systems.

Heavens then transitioned to climate-related risks, emphasizing that the impact on financial institutions is more about financial system vulnerabilities than direct natural hazards. He presented two scenarios: an extreme seasonal drought in Europe and a catastrophic sea-level rise due to Antarctic ice sheet collapse. Both scenarios demonstrated how climate events can disrupt economic stability, but the response from financial institutions may be muted due to perceived manageability or confidence in handling such crises.

Heavens concluded that financial institutions must link climate risk with sovereign debt and insurance issues. He called for better predictability and early warning systems, particularly regarding ice sheet collapse and ocean monitoring, to ensure financial stability and effectively mobilize private capital for climate adaptation and mitigation efforts. Heavens stressed the need for granular impact assessments and improved decadal predictability to create a virtuous cycle of risk management and investment in climate resilience.

Stress testing in the context of supply-chain resilience and financial-sector resilience

Mark Flood, *University of Maryland*

Mark Flood presented on stress testing as a cornerstone of financial supervision and risk management, particularly after the financial crises of the 1980s, 1990s, and the 2008 global financial meltdown. Flood outlined the evolution of stress testing from its initial applications in financial systems to its current use in analyzing supply chains and other sociotechnical systems. He explained that stress testing involves conditional forecasting where scenarios are modeled to anticipate potential disruptions and evaluate system responses. He introduced two primary methods of stress testing: forward stress testing, which simulates stress events on a system model to observe outcomes, and reverse stress testing, which identifies potential scenarios that could lead to unacceptable outcomes.

Flood highlighted the importance of these techniques using practical examples. For instance, in financial contexts, he shared that forward stress testing might involve simulating market disruptions on financial portfolios, while reverse stress testing might identify vulnerabilities that could lead to severe financial losses. Flood noted the discussion extends to the use of stress testing in supply chain management, emphasizing its role in improving situational awareness and resilience.

Flood also touched on the integration of stress testing into cyber-physical systems and the challenges of adapting these methods for complex, interconnected environments. He concluded with a call for ongoing development and refinement of stress testing frameworks to address emerging risks and complexities in various domains.

The challenge of adaptation seen through the lens of complexity

Giovanni Fusina, *Defence Research and Development, Canada* and Enda Murphy, *National Research Council of Canada*

Giovanni Fusina described the characterization of complex systems as having interdependent components whose interactions give rise to emergent behaviors, phase transitions and evolution. Unlike traditional reductionist approaches that isolate individual elements, Fusina explained how complex systems science examines the collective behaviors that arise from the relationships between a system's parts. He shared that techniques used in this field include cellular automata, graph theory, chaos theory, dynamical systems

and statistical mechanics. Fusina noted recent Nobel laureates Manabe, Hasselmann and Parisi as having enhanced our understanding of climate change through complex systems methodologies.

Fusina observed that adaptation to climate change necessitates interventions designed to reduce risk. One useful concept from complex systems science he shared is the complexity profile, which measures the behaviors a system can achieve at different scales. Fusina described Ashby's Law of Requisite Variety that states that a system must be as complex as the environmental behaviors it needs to address to be effective. He noted this principle is refined for multi-scale systems, suggesting that the system's complexity at all scales must exceed the environmental complexity.

Fusina presented coastal flood adaptation as a practical application of this concept. Traditional methods, like sea walls, he noted are high in scale but low in complexity, as these methods are designed for specific conditions and fail if those conditions are exceeded. Conversely, he detailed, nature-based solutions like those developed by the U.S. Army Corps of Engineers mimic natural processes and structures, incorporating various environmental and societal factors. Fusina expressed that while high in complexity, these solutions may have lower scale applicability, necessitating hybrid approaches that combine nature-based and hard infrastructure to handle greater sea level rises effectively.

Fusina also talked about applications of complex systems science to other adaptation initiatives, such as wildfire management and water resource availability. He noted these problems involve multiple compounding effects and require comprehensive strategies that account for various interacting factors. By leveraging the tools and principles of complex systems science, Fusina argued that more robust and adaptable solutions can be developed to address the multifaceted challenges posed by climate change.

Policy response to climate and the role of community representatives

David Kaufman, *CNA*

David Kaufman explored using ecosystem models to understand and manage the complex interrelationships among multi-sectoral actors in real-world communities. Kaufman presented the central challenge as navigating the intricacies of governance and mobilizing efforts across public, private and civic sectors, each with distinct but overlapping interests. Drawing from biological and business ecosystem models to address these challenges, Kaufman proposed a framework that categorizes stakeholders into four types: builders, pioneers, transactors and specialists.

Kaufman described builders as large, well-connected organizations that leverage resources to implement solutions on the ground. He noted that pioneers focus on novel approaches to problems and are often grassroots organizations. He pointed to transactors as stakeholders who provide necessary resources but may lack connections to local entities. Specialists, he summarized, possess advanced knowledge and research capabilities.

Kaufman highlighted a case study from New Orleans, Louisiana, United States, that applied this framework to climate change adaptation efforts. By mapping and categorizing 77 projects and their associated actors, the study revealed gaps and connectivity issues in the network, such as the lack of integration of key entities like the Louisiana Climate Initiative Task Force. Overall, he emphasized the approach's focus on the visualization and balancing of actor types to address complex, cross-sectoral issues effectively. Kaufman advocated for integrating these insights into policy frameworks to better manage interconnected challenges.

National critical infrastructures: The need for addressing cascading effects and cross-sector governance

Jonas Johansson, *Lund University*

Jonas Johansson presented on critical issues related to cybersecurity and crisis management, focusing on the interdependencies of critical infrastructures and their societal impacts at various levels — from local to international. Johansson highlighted the importance of governance and management in securing these infrastructures and adapting them to climate change and hybrid threats.

From a European and Swedish perspective, Johansson reviewed existing frameworks for national risk assessment and civil preparedness, such as the European Entities Resilience Directive and NATO's baseline requirements. He underscored Sweden's emphasis on national capability for cross-sectoral analysis of interdependent infrastructures, particularly in the context of supply security and defense.

In terms of climate adaptation, Johansson expounded on risks like local scour of bridge foundations, which vary with climate change projections. He emphasized the need for research into local adaptation models, infrastructure impacts, and future design considerations.

Johansson also explored how national critical infrastructure affects supply chain resilience, and the interconnectedness of the two, such as disruptions in transportation impacting accessibility to diesel and grain. He noted the necessity of data to analyze interdependencies and cascading effects, using examples like the pandemic's impact on interdependent societal functions and heavy rainfall disrupting power systems and railway operations.

Finally, Johansson proposed a new meso perspective — focusing on intermediate levels of functions and flows — over existing micro or macro views. He introduced the JEDI-CI initiative, a collaborative project between DHS CISA and the Swedish Civil Contingencies Agency, as a framework for the joint exchange of data to improve risk management and cross-sector resilience.

Climate change, security, and misinformation

Tom Ellison, *Center for Climate and Security*

Tom Ellison presented recent work on climate change, security and misinformation, arguing for the expansion of the scope beyond the common associations with fossil fuel marketing or climate denialism. Ellison introduced a broader framework that explores how climate change and its impacts create opportunities for misinformation, affecting security and stability.

He explained the framework distinguishes between misinformation or the unintentional spread of falsehoods, disinformation or the deliberate spread of falsehoods, and malinformation or the misleading presentation of true information. Ellison gave as an example of malinformation a Facebook page highlighting migrant crime, misrepresenting the broader truth that migrants don't commit more crimes than native citizens in the U.S.

Ellison outlined climate change's direct impacts, such as extreme weather and its implications for infrastructure and populations, and the security risks associated with these impacts. He discussed the social and political cascades from these physical risks, such as xenophobic backlash to migration or increased military involvement in disaster relief. Additionally, he noted how response risks arise from climate policies, which, while necessary, can destabilize petrostates or lead to land use conflicts. Ellison highlighted examples of misinformation exacerbating these risks, such as states blaming adversaries for climate disasters or exploiting policy reactions to sow discord. He specifically cited the 2023 Maui, Hawaiʻi wildfires, where China and Russia spread disinformation to manipulate public perception.

Ellison emphasized the need for resilient climate policymaking that anticipates misinformation's role in exacerbating climate risks. He called for more cohesive discussions on climate misinformation in policy circles, drawing parallels with robust conversations around vaccine misinformation and election security. He shared the goal is to design and communicate policies that mitigate both the perceived and real impacts on affected populations, ensuring a just energy transition.

Beyond the trend: The superposed impacts of climate change and variability on cyberinfrastructure

Christina Karamperidou, *University of Hawai'i at Mānoa*

Christina Karamperidou discussed the challenges posed by climate change and cyberattacks on data centers. Karamperidou described how modern data centers often use economizers in their cooling infrastructure, which bring in outside air to help cool their equipment while reducing energy consumption. However, she noted increasing frequency and intensity of hot and humid conditions due to climate change threaten the reliable operation of these data centers. She shared how deadlines frequently highlight data centers shutting down or overheating during heatwaves, events that are becoming more common.

Karamperidou stressed the significant threat cyberattacks pose by targeting cooling management systems, which often have weaker cybersecurity compared to other components of data centers. She explained these attacks can weaponize heat, making data centers in hot and humid regions or during summer particularly vulnerable. She cited the 2019 attack on an Iranian data center related to its nuclear program and missile launch systems, where components of its cooling system were allegedly manipulated to cause a shutdown.

Karamperidou highlighted the dual threat of climate-induced heatwaves and cyberattacks, which can disrupt services, trade, national security, and cause social unrest. She gave the heatwaves of 2022 as an example where data centers in London and Sacramento were knocked offline due to extreme heat. She commented on how this issue is exacerbated by the fact that most existing data centers were designed based on historical climate information and are now facing unprecedented temperature extremes.

She acknowledged the interplay between climate change and climate variability, particularly events like El Niño and La Niña, further complicates the situation. Karamperidou reported these climate phenomena can exacerbate heat and humidity risks, affecting the efficiency of cooling systems and increasing the vulnerability of data centers to overheating and cyberattacks.

To address these challenges, Karamperidou emphasized the need for better prediction of El Niño and La Niña events and consideration of both climate trends and variability in future assessments. She stated the goal is to improve resilience through technological advancements and more robust cybersecurity measures for cooling management systems.

Improving global security, deterrence and defense: Cyber-physical-social systems and climate change nexus perspectives

Rossitza Homan, Sandia National Laboratories

Rossitza Homan argued that to improve security, deterrence and defense we must consider how climate impacts exacerbate existing threats and create new risks to interdependent cyber-physical-social and natural systems. Homan encouraged participants to think about how extreme weather events, sea-level

rise, and shifting climate patterns impact cyber-physical-social systems, economic stability, and geopolitical dynamics.

Homan discussed Sandia's comprehensive approach to climate modeling, infrastructure modeling and the impacts of various threats on interdependent infrastructures. She described how Sandia, as a federally funded research and development center, not only develops scenarios and models threats but also recommends mitigation and adaptation strategies.

Homan focused on innovation within the context of security, deterrence and defense, emphasizing Sandia's primary mission of securing critical systems across the nation and ensuring global security due to interdependencies among cyber-physical-social and natural systems. Homan highlighted the evolving nature of threats since Sandia's establishment 75 years ago, pointing out significant changes, such as the collapse of the Soviet Union, the rise of cyber threats and the militarization of space. She reiterated that addressing global security, deterrence and defense challenges in this complex, multipolar landscape with diverse and interconnected threats requires improving the resilience of cyber-physical-social systems to both manmade and natural disruptions.

Homan moved to the example of the recent CrowdStrike incident, illustrating the potential for cascading effects from cybersecurity breaches on physical and social systems. She reflected on how that incident underscores how even well-established cybersecurity firms could inadvertently cause cascading disruptions to cyber-physical-social systems and the potential for malicious actors to exploit such vulnerabilities intentionally.

Homan addressed the energy consumption and environmental impact of data centers, particularly in the context of AI and large-scale data processing. She called for greater transparency in understanding and mitigating the environmental impacts of computing resources. Homan also touched on the cybersecurity vulnerabilities of electric vehicle charging stations, highlighting the need for foresight in deploying new technologies. While EVs represent a positive step towards reducing emissions, she called for more secure support infrastructure to prevent potential cyberattacks that could disrupt charging networks and compromise vehicle safety.

Homan asserted the need for effective research-to-deployment pipelines to improve global security, deterrence and defense. She also recognized that implementing resilience solutions in real-life is challenging because it involves a multi-stage process and requires effective partnerships across R&D-government-industry organizations and local communities. Homan called attention to the need for innovation and new ways of thinking to bridge the gap between research and operational deployment, overcoming the "valley of death" in translating promising research into real-world solutions. She stressed the importance of collaboration among research and operational organizations to address the growing and evolving challenges in national and global security.

Panel Discussion with Presenters

Igor Linkov, *U.S. Army Engineer Research and Development Center*
Lilian Alessa, *University of Idaho*
Facilitator: Marthie Grobler, *CSIRO*

Marthie Grobler led a panel with the short talk presenters and two additional workshop presenters, Igor Linkov and Lilian Alessa. In response to Grobler's first question on the most concerning climate change impacts for social, cyber and physical systems, panelists named migration and social science gaps. For migration, the concern was focused on how climate change could drive migration, with impacts to

housing and security. Panelists also points to gaps in understanding the social science aspects of climate change, especially regarding authoritarian responses to climate impacts and their social consequences.

Grobler's second question asked for strategies and actions to characterize and manage the risks to social, cyber, and physical systems. Panelists described the need for higher-resolution models at the local and human scale to better understand and manage climate risks. These advances would require enhanced data collection and monitoring. Panelists also noted that effective risk management will require increased access to existing data through international cooperation and interdisciplinary collaboration.

When asked about the most pressing research and development needs, panelists gave answers in five main categories: relevance of data, interdependencies and resilience, paradigm shifts, operational social science, and ocean and cryosphere data. Despite data being abundant, panelists noted the data often lack relevance to current decision-making needs. They called for more R&D to frame the needs of decision-makers to ensure data relevance. Panelists noted the need to build awareness of and address interdependencies and resilience more effectively. They suggested a shift in thinking about adaptation solutions, moving beyond outdated technologies and embracing innovative approaches. Panelists called on social science research to improve in forecasting and understanding human behaviors and perceptions related to climate change. They posited that low-cost observation networks could provide valuable data. Lastly, panelists shared that managing large volumes of ocean and cryosphere data requires advanced systems.

When asked how we could partner differently, panelists pointed to the need to educate stakeholders about the climate nexus and fostering collaboration across various organizations. They agreed that integrating major systems and standardizing data terms could enhance effectiveness.

Panelists suggested that on way to deal with the current polycrisis as it extends into the political sphere is to focus social science on bottom-up interactions and to effectively channel data to decision-makers. While formal governance structures are important, the panelists point out that much of the action occurs informally, emphasizing the need to build resilient landscapes. When thinking about migration, for example, panelists noted the criticality of interdisciplinary approaches. They argued for the adaptation of social science into practical decision-making and the integration of basic knowledge with specific questions to enhance resilience and solidarity.

Day Three

Introductory Talk

From threat multiplier to opportunity multiplier in climate security and *infrastructure resilience*

Sherri Goodman, Wilson Center

Sherri Goodman recounted her professional journey and the intersection of climate change with national security. Goodman began by reminiscing about her early days on the Senate Armed Services Committee during the Cold War, highlighting her involvement with the Department of Energy's Nuclear Weapons Complex and the oversight of various nuclear facilities.

Transitioning from the Cold War era, she discussed her tenure as the first Deputy Undersecretary of Defense for Environmental Security from 1993 to 2001. During this period, she witnessed the military's initial foray into environmental issues, focusing on compliance with environmental laws and the conservation of natural resources. She then pivoted to her work at the Center for Naval Analysis, where in

2007, she led a pioneering group of military leaders to evaluate the security implications of climate change, coining the term "threat multiplier" to describe its impact.

Goodman emphasized the evolving recognition of climate change as a significant national security issue, noting how the discourse has shifted from purely scientific to encompass broader geopolitical and operational dimensions. She also addressed the compounded risks posed by climate change, such as droughts, wildfires, sea level rise and extreme weather events, and how these interact with other factors like poverty, governance and demographics to exacerbate instability.

Sherri introduced her forthcoming book, "Threat multiplier: Climate, military leadership, and the fight for global security," which chronicles the military's growing awareness and response to environmental challenges. She explained that the book aims to provide a comprehensive historical perspective on these issues, underscoring the importance of integrated risk assessment and resilience planning in contemporary defense strategies.

Science of Analytical Gaming

Lynn Yang

Lynn Yang gave an introduction on traditional and analytical wargaming, highlighting their uses, limitations and advancements in the field. Yang explained traditional wargames, used for training and policy analysis at institutions like the Naval War College, involve dynamic conflict simulations where players make decisions and respond to outcomes. However, she noted these games are often experiential, with potential biases, limited runs, qualitative data and proprietary designs, restricting their replicability and generalizability.

To address these issues, Yang introduced workshop participants to analytical gaming, which integrates experimental sciences with wargaming to create a more rigorous and data-driven approach. She articulated that analytical games, unlike traditional wargames, are designed to be repeatable, data-generative, and methodical. Yang noted these games attempt to balance the flexibility and exploratory nature of wargaming with the control and statistical rigor of experimental research. She shared this approach is particularly valuable in complex problem spaces with sparse data, such as nuclear deterrence, where real-life observational data is limited.

Yang then provided an example of such an analytical game, "Signal," which explores the impact of tailored nuclear weapons on nuclear escalation. She walked participants through the game, which can be played both as a board game and online and simulates crisis scenarios where players manage resources and respond to crises to achieve objectives. She related that the game has been played extensively, generating data that suggests tailored nuclear weapons do not significantly impact escalation, although this finding needs to be corroborated with other data sources.

Yang emphasized that while analytical games are not a standalone solution, they complement traditional wargames by providing deeper insights into specific research questions. She explained the development of these games involves collaboration with experts in game theory and mathematics to optimize the game design for meaningful data collection. Yang concluded with an example of a game developed for NATO to study consensus-making under crisis, illustrating the broader applicability and potential of analytical wargaming in various domains.

Short Talks

Modeling human dynamics for critical infrastructure resilience

Budhendra (Budhu) Bhaduri, Oak Ridge National Laboratory

Budhendra Bhaduri presented on the complexities of human interaction with infrastructure and how individual decisions at a micro-scale can lead to significant macro challenges such as traffic congestion, pollution, and public health impacts. Bhaduri noted these issues often arise from human behaviors, as people frequently move for convenience rather than necessity. Bhaduri focused his presentation on climate change induced displacement and migration as one of the most anticipated changes in the global human landscape.

Bhaduri recounted that the movement of people presents various problems, including the risk of encountering unprepared hazards, starting wildfires that necessitate evacuations, and suffering heat-related deaths during heatwaves. He emphasized the importance of forecasting population movements across different time horizons for mitigating natural hazards and saving lives, whether through rapid evacuations during natural disasters or addressing climate migration.

However, as he shared, forecasting population movements remains a complex issue. He noted, for example, that understanding migration as a consequence of sea level rise from climate change requires a comprehensive assessment of global shoreline and coastal area changes and loss of human habitat and displacement. He suggested tools, such as the Landscan and LandCast population models, can help assess and forecast human distribution and redistribution patterns. By simulating population distribution and dynamics, he explained these models aid in identifying possible future intersections of human settlements and hazards, and infrastructure vulnerabilities. He noted that this work would allow for strategic planning to minimize impacts on both infrastructure and human safety.

Is cybersecurity turning up the heat on climate change?

Helge Janicke, Cyber Security Cooperative Research Centre, Australia

Helge Janicke discussed the intersection of cybersecurity and climate change, emphasizing the potential for cyber threats to exacerbate the impacts of climate change. Janicke expressed concerns that as society increasingly relies on technology to address climate issues, vulnerabilities in these technologies could be exploited by various adversaries, including disillusioned individuals, organized criminals and nation-states. He highlighted that the increasing dependence on technology, such as cooling systems and renewable energy infrastructure, creates new opportunities for cyberattacks, which could have severe consequences, especially during critical times like heatwaves. He also stressed the importance of ensuring the security of technological solutions and supply chains, particularly in the context of renewable energy initiatives like rooftop solar installations. He concluded by urging caution in the rapid deployment of technology to address climate change, warning that threat actors and cyber vectors will continue to evolve alongside these changes.

Human-centered cyber security

Giovanni Russello, Auckland University

Giovanni Russello discussed vulnerabilities and human errors in cybersecurity incidents, using an example like CrowdStrike to illustrate how mistakes can lead to exploitation. Russello emphasized that both technical flaws and human errors contribute to these issues. He used the analogy of the evolution of

cars to highlight that while modern systems aim to enhance productivity, they often fail to incorporate assistive technologies to mitigate human errors. As a result, he noted, some of these tools are comparable to cars designed 100 years ago, which provided minimal support to drivers and led to numerous accidents due to poor design rather than direct human error.

He then focused on phishing, a type of social engineering attack where attackers manipulate human emotions to achieve their goals, often leading to data breaches or ransomware attacks. Russello described phishing as distinct from spam as it involves attackers impersonating legitimate entities to build trust. Despite growing awareness and technological solutions, he observed that phishing remains highly effective, costing the global economy over $20 billion annually.

Russello explained that current anti-phishing strategies are categorized into technical solutions, like filtering and anomaly detection, and training programs. He shared that both approaches have limitations; technical solutions can't catch all threats, and awareness campaigns alone aren't sufficient. Russello argued that humans are the last line of defense and need better support during interactions with potentially malicious emails.

Russello presented research focused on understanding susceptibility to phishing. Summarizing a review of the past decade's research, he described three categories of variables that influence susceptibility: stable long-term factors like demographics, situational variables like devices used to access email, and immediate factors like cognitive reactions. Russello highlighted a research gap in the situational variables category, suggesting it offers opportunities for intervention.

Russello also explored the role of biometrics in assessing susceptibility, positing that factors like stress and lack of sleep could predict vulnerability to phishing. He shared results of a study that manipulated workload and found that high-stress conditions increase susceptibility, especially to relevant phishing emails. He concluded that this research underscores the need for personalized interventions based on an individual's context and state.

Three worldviews for complex systems

Thushara Gunda, Sandia National Laboratories

Thushara Gunda addressed the multifaceted nature of climate security challenges, initiating her presentation with a movement exercise to emphasize the complex interplay of natural, built and social systems in addressing climate security. Gunda a complex systems analyst at Sandia, examined these perspectives to understand and solve climate-related issues. Gunda defined climate security as the impact of climate change on peace and security, particularly in fragile and conflict-affected areas. She noted that it encompasses exacerbated food and water insecurities, prolonged conflicts and disruptions to social and national systems. Gunda referenced a U.S. national intelligence estimate that highlights various drivers of climate security concerns, including resource competition, social disruptions and displacement.

Gunda described how climate security issues can be framed using three primary worldviews: environmental resources, infrastructure resilience, and regional dynamics. She explained that concurrent consideration of all three worldviews is essential for contextualizing and assessing climate security issues comprehensively. Gunda argued that considering all three perspectives concurrently can lead to more meaningful assessments and operational strategies.

Gunda then shared a case study in the energy sector to illustrate the application of these worldviews. She presented two major questions facing the energy sector: maintaining reliable energy production and transitioning to decarbonized systems. Considering these questions, she noted the environmental perspective involves understanding the impacts on energy systems of natural system changes like droughts and extreme weather. She commented that infrastructure resilience focuses on the ability of

current and planned systems to withstand these changes, while regional dynamics consider social influences and behavioral changes impacting energy systems.

She explained the integration of these worldviews facilitates a holistic approach to climate security, recognizing the interconnectedness of natural, built, and social systems. Gunda highlighted the importance of breaking down silos between disciplines and operational thinking to address co-occurring climate security concerns, such as migration, infectious diseases and cyber-physical interactions. She finished her presentation by urging for the development of robust mitigation strategies that consider the complex, interconnected nature of climate security challenges.

Banquet TED-style Talks

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

Malcolm Mistry started his presentation noting that by 2050 an additional one billion people are projected to live under extremely high-water stress, defined as over 80% stress, caused by increased demands from irrigation, livestock, energy, population growth, data cooling and manufacturing. Mistry pointed to climate change as exacerbating this issue by affecting water security and agricultural productivity, leading to cascading impacts on conflict risk and migration, which in turn hinder adaptation and mitigation efforts.

Mistry commented that melting glaciers pose additional threats, exemplified by the Camp Century site, a former US military base designed as a launch site, subsequently abandoned and buried under ice. As glaciers melt in a warming climate, he noted contaminants could enter the ecosystem, with similar risks present at other global sites, such as in parts of Scandinavia as a result of the fallout from the Chernobyl disaster.

Mistry pointed out prolonged periods of low wind speeds, described as a "wind drought," cause offshore wind farms to underperform. He surmised this underperformance may have spillover effects on renewable energy security and financial lending institutions in future, highlighting the interconnected nature of environmental changes, energy and economic stability.

Climate adaptation decision-making

Robert Kopp, Rutgers University

Robert Kopp presented on benefit-cost analysis, a process commonly used by agencies like the Army Corps that assumes reasonable probability distributions of outcomes to value the consequences of different planning choices. However, as Kopp noted, quantifying climate risks is complex, often involving non-linear changes and unknown likelihoods. Despite this uncertainty, he asserted decisions on topics like infrastructure planning and land-use, with time horizons lasting many decades, must be made.

Kopp contended dynamic adaptive policy pathways offer a method for adaptive decision-making, based on contingency planning and the identifications of triggers for switching between policy levers. However, he observed uptake of this approach in the United States has been limited, possibly due to disaggregated nature of adaptation decision making and uncertainty about long-term budgets and political will.

He argued effective climate adaptation requires the integration of decision science, political science and institutional frameworks. Kopp identified challenges to include identifying responsible actors, navigating a climate of low trust and dealing with democratic backsliding. Without addressing these coordination and implementation issues, he expressed adaptative approaches to adaptation planning may not be successful.

Infrastructure resilience as a social process: Domain awareness

Lilian Alessa, University of Idaho

Lilian Alessa presented on Socially Integrated Infrastructure Planning, which incorporates local communities and place-based knowledge to enhance infrastructure resilience. Alessa shared that this approach, which emphasizes place over race, is crucial for maintaining resilient functions, especially in remote areas. She noted Community-Based Observing Networks have been developed for SIIP to address vulnerabilities in changing environments. She explained these networks leverage intimate place knowledge to establish baselines, detect deviations and improve community cohesion and relationships with state and federal entities.

Alessa communicated that CBONs can collect observational data, identify indicators, create geographic information system layers, produce maps and generate precise data. She revealed CBONs have been effectively used on the Russian border, providing a two-year early warning for seal wasting disease. She noted that CBONs adhere to best practices to ensure repeatable and endorsed standards. She noted the versatility of these networks makes them applicable to energy and infrastructure projects.

Alessa pointed out that CBONs can operate in areas where traditional sensors fail, providing unparalleled data with context, imagery and precision. She shared how CBONs benefit communities by enhancing social capital, enriching STEM programs and fostering community cohesion. She used the Greenland/Danish defense CBON — Kalaallit Nunaata Alapernaatsui — as an example that exemplifies effective implementation. She also noted that High Fidelity Observers ensure the reliability and contextual relevance of the data collected.

UK Ministry of Defence efforts at the CPSICC nexus

Honor Sangster, UK Ministry of Defence

Honor Sangster presented on the United Kingdom Ministry of Defence's efforts at the CPSICC nexus. First, Sangster shared the UK is conducting a Strategic Defence Review that will determine the roles, capabilities and reforms required by UK Defence to meet the challenges, threats and opportunities of the twenty-first century. She then noted the Infrastructure Directorate is responsible for estate policy and strategy, and has recently developed an Estate Climate Resilience Plan. She explained the U.K. MOD has a well-established methodology for assessing climate risks to the operation of establishments developed in collaboration between climate change resilience experts and site-level personnel, such as facilities managers. She discussed how the U.K. is supporting NATO Allied Command Transformation in developing a layered resilience concept by sponsoring the Military Infrastructure Thematic Working Group. Sangster described how Sangster described how the military infrastructure component of the concept recognizes climate change as a threat and sets out recommendations to improve NATO and Allied Nations resilience to climate change.

Waste heat is an inexplicably neglected environmental problem and at the same time an unused energy treasure

Fero Simancik, Slovak Academy of Sciences

Fero Simancik started his presentation by noting the significant rise in global temperatures over the past century, which is largely attributed to human activity. Simancik explained that without human influence, solar energy reaching the Earth is mostly reflected and radiated back into space at night, and only partially stored in photosynthesis and land formation. He noted this energy balance established over the past millions of years has led to a stable global surface temperature for a long time. However, as he pointed out, man-made burning of fossil fuels brings additional heat into the atmosphere and simultaneously increases the greenhouse effect, which worsens its radiation into the surrounding space. He described how this additional heat energy trapped in the Earth system then leads to the unwanted global warming observed today.

In fact, as Simancik surmised, all forms of energy used by humans are ultimately converted into heat, even those produced from renewable primary energy sources. He noted this additional heat triggers more natural CO_2 emissions, such as from the oceans, causing a cascading increase of the global temperature the atmospheric CO_2 content. To mitigate this effect, he argues it is therefore necessary to reduce not only CO_2 emissions but also the total amount of human-generated heat. He proclaimed this approach viable because use a significant part of the converted primary energy is currently thrown away without any use as waste heat.

With the help of innovative heat batteries and efficient heat exchangers, he contended it is technically relatively easy to capture and store waste heat and use it for heating or air conditioning of households. Considering that additional heat in the atmosphere is also generated by use of electrical energy, he expressed an urgent need for a new sustainable energy strategy for humanity, consisting rather of a higher efficiency in the use of primary energy, instead of excessive electrification at any cost.

Climate risks to critical infrastructure

Matteo Gerlini, University of Siena

Matteo Gerlini gave a taped presentation the vulnerability of critical infrastructure systems to climate change risks. He discussed how higher temperatures reduce system efficiency and increase demand for energy and infrastructure. To mitigate these risks, Gerlini stated that it is essential to develop resilient systems with robust response capabilities and integrate climate planning into infrastructure considerations. He asserted the critical need to build redundant and flexible systems to avoid single points of failure.

Gerlini recommended the implementation of nature-based solutions, which offer additional benefits but cannot be universally applied. He asserted that engaging local communities in resilience strategies and encouraging their participation ensures the tailoring of solutions to specific needs and vulnerabilities. He called for immediate and sustained attention to these issues, along with a change in attitude.

Additionally, Gerlini highlighted small modular nuclear reactors as a necessary component for transitioning to a secure and resilient cyber system. Overall, he called for a multifaceted approach to enhance the resilience and reliability of critical infrastructure amidst evolving climate challenges.