



The Pearson Global Forum

**PEARSON GLOBAL
FORUM REPORT**
October 12-14, 2021



.....

The Pearson Global Forum

.....



Note of Welcome from the Institute Director

On behalf of The Pearson Institute for the Study and Resolution of Global Conflicts, I'd like to welcome you to The Pearson Global Forum, *Information in Conflict*. This paramount (virtual) gathering has brought together scholars, leaders, and practitioners to address pressing issues of global conflict through the sharing of data-driven research on current and past aspects of conflict and the identification of important lessons for conflict resolution from around the world.

The Pearson Institute for the Study and Resolution of Global Conflicts was established through a grant from the Thomas L. Pearson and Pearson Family Members Foundation and is dedicated to contributing to a world more at peace through research, education, and engagement. As an institute within the Harris School of Public Policy, our distinguished faculty apply a data-driven, analytical approach to examining issues related to conflict and reconciliation and are currently working in Nigeria, Afghanistan, and Colombia, among other countries. Through our Fellows and Scholars program for master's and doctoral students and our course curriculum, we hope to inspire future policy leaders and academics to focus on these topics in a rigorous way.

It is our goal to convene leading scholars and high-level policy makers from around the globe to exchange ideas and maximize the potential for impact in preventing and resolving violent conflicts and informing policy. We hope this Forum is an opportunity for you to learn of current research and active endeavors to promote peace through conflict resolution, and begin important conversations that may impact positive change. I'd like to extend my personal thanks to you for joining us, and I welcome you to our virtual Pearson Global Forum.

Sincerely,

James Robinson

*Institute Director, The Pearson Institute;
The Reverend Dr. Richard L. Pearson Professor
of Global Conflict Studies and University Professor,
Harris School of Public Policy and Department of Political Science,
The University of Chicago*



The Pearson Global Forum

In October 2021, the University of Chicago's Pearson Institute for the Study and Resolution of Global Conflicts presented the fourth annual Pearson Global Forum, *Information in Conflict*. This Forum is a significant public event with the goal of convening leading scholars and high-level policy makers from around the globe to exchange ideas and maximize the potential for impact in preventing and resolving violent conflicts and informing policy. This conference discussed the causes and consequences of conflict, and strategies to intervene and mitigate conflict and to consolidate peace.

The knowledge that forms the foundation of our understanding, decisions, advancement, and the world is now in question. Scientific fact and proven theorem are being set aside for apocryphal beliefs. The emergence of new conflicts is outpacing the ability of the international community to cope, new rules now govern old disputes, disunity through the spread of populism is creating long-term damage, and disinformation and the abuse of knowledge are taking a devastating toll on our global world. As the international community continues to deal with dozens of active conflicts, and the quickly shifting relationships between and among nations, it essential to find paths towards resolution, peace, and stability.

At The Pearson Institute, we are mobilizing our mission to convene international leaders and world-renowned academics at The Pearson Global Forum to explore rigorous research and analysis to influence solutions, strategies, and policy for reducing and mitigating conflict to achieve a more peaceful world.

The Pearson Institute for the Study of Global Conflicts

The Pearson Institute for the Study and Resolution of Global Conflicts at the University of Chicago promotes the ongoing discussion, understanding and resolution of global conflicts, and contributes to the advancement of a global society more at peace. Established through a gift from The Thomas L. Pearson and The Pearson Family Members Foundation, and led by Institute Director James Robinson, co-author of *Why Nations Fail* and *The Narrow Corridor*, the Institute achieves this by employing an analytically rigorous, data-driven approach and

global perspective to understanding violent conflict. It is global in its scope, activities and footprint, attracting students and scholars from around the world to study conflict and new approaches to resolution.

The University of Chicago

The University of Chicago is a leading academic and research institution that has driven new ways of thinking since its founding in 1890. As an intellectual destination, the University draws scholars and students from around the world to its home in Hyde Park and campuses around the globe. The University provides a distinctive educational experience, empowering individuals to challenge conventional thinking and pursue research that produces new understanding and breakthroughs with global impact. Home to more than 90 Nobel laureates, the University of Chicago is dedicated to an environment of fearless inquiry and academic rigor.

**THE PEARSON INSTITUTE
FOR THE STUDY AND RESOLUTION
OF GLOBAL CONFLICTS**

1307 East 60th Street, Chicago, IL 60637

-  thepearsoninstitute.org
-  thepearsoninstitute@uchicago.edu
-  +1 773 834 3652
-  ThePearsonInstitute
-  PearsonInst
-  bit.ly/2SZN4Kn
-  linkedin.com/company/the-pearson-institute

WRITTEN BY: Sheila Kohanteb
EDITED BY: Sheila Kohanteb and Alex Carr

PHOTOS • Front cover and page 1: People looking at newspapers on a wall in Yazd, Iran. Photo by BalkansCat, iStock • **Pages 6–7:** Network Earth, artwork by geralt, Pixabay • **Page 8:** Earth Internet, artwork by TheDigitalArtist, Pixabay • **Page 26:** Young Saudi women using smart phones at their college. Photo by Alessandro Biascioli, iStock • **Pages 36, 53 and back cover:** Terminal display warning about a cyber attack, artwork by matejmo, iStock

DESIGN AND LAYOUT: Josh Babcock and Agency EA.

DISCLAIMER: The views expressed in this document do not necessarily reflect the views of The Pearson Institute for the Study and Resolution of Global Conflicts nor the University of Chicago. Where the text refers to statements made by participants at The Pearson Global Forum, every effort has been made to provide a fair representation of their views and opinions.



Contents

- 2 Note of Welcome from the Institute Director
- 4 About the Pearson Global Forum, Pearson Institute, and University of Chicago

TUESDAY, OCTOBER 12, 2021

- 9 Welcome Remarks: James A. Robinson
- 10 Keynote | Own Your Data: Taking Control of Our Digital Future
- 12 Panel | Manipulating Knowledge
- 14 Flash Talk | Misinformation: Why Is It a Problem?
- 16 Panel | Impact of Social Media on Global Affairs
- 18 Flash Talk | Facebook Causes Protests
- 20 Keynote | The Future of Yemen
- 22 Case Study | Yemen in Neglect
- 24 Flash Talk | Gang Rule

WEDNESDAY, OCTOBER 13, 2021

- 27 Welcome Remarks: Katherine Baicker
- 28 Case Study | Iran
- 30 Flash Talk | Russia's Firehose of Falsehoods
- 32 Case Study | Saudi Arabia
- 34 Flash Talk | Comparative Constitutionalism: Islam in Perspective

THURSDAY, OCTOBER 14, 2021

- 37 Welcome Remarks: Ka Yee C. Lee
- 38 Keynote | Constant Confusion: Technology Meets Modern Conflict
- 40 Panel | Artificial Intelligence and International Security
- 43 Fireside Chat | AI, War, and National Security
- 45 Flash Talk | Trends and Insights from the Ransomware Ecosystem
- 47 Panel | Cyber Abuse, Security, and Defense
- 49 Flash Talk | The Quantum Revolution: A New Paradigm for Communication
- 51 Participation Infographics



Welcome Remarks

James A. Robinson

*Institute Director, The Pearson Institute;
Reverend Dr. Richard L. Pearson
Professor of Global Conflict Studies and
University Professor, Harris School of Public Policy and
Department of Political Science,
The University of Chicago*

James Robinson introduced the 2021 Global Forum, Information in Conflict, and explained that “The Pearson Institute was founded on an approach of deep-diving into different parts of the world and try[ing] to understand the specifics of the problems and culture to understand the roots of conflict and how to resolve them.” The Forum creates a space where academics, policymakers, private sector voices, and civil society practitioners can understand the determinants of conflict in an increasingly digitized world. As groups become incentivized to use artificial intelligence (AI) to influence populations and economic gain, the effective institutional design will require collaboration and empirical data.

Tuesday, October 12, 2021



KEYNOTE

Own Your Data: Taking Control of Our Digital Future

Brittany Kaiser

Co-Founder, Own Your Data Foundation;
Cambridge Analytica Whistleblower

Opening the first day of the 2021 Pearson Global Forum, Brittany Kaiser discussed current personal data privacy practices. Kaiser believes that increasing the public’s digital intelligence is imperative to creating a moral, transparent, and consensual global future. While there has been an significant increase in digital data due to the COVID-19 pandemic, there is a worldwide need for cohesive protections against the monetization of data, and sanctions for those who disregard those protections. To achieve a more comprehensive data privacy regime on a national and global level requires a higher level of understanding of how personal digital data is monetized. Quoting *The Economist*, Kaiser emphasized how valuable information is, calling it “more valuable than oil and gas.”

Both private and public corporations purchase and use personal data to develop business, military, and public policy strategies. In recent years, the world’s largest companies have all developed expertise in deriving additional value from private data gathered from their customers. The population of the world is producing assets that are bought, sold, and traded globally for

trillions of dollars, yet the producers of these valuable assets have no rights. Kaiser explained that few users read the terms and conditions of privacy policies and emphasized the lack of explicit understanding of what users agree to; users thus cede the power of their data to these companies.

Kaiser, a Cambridge Analytica Whistleblower, is co-founder of the Own Your Data Foundation, which trains people to be more digitally intelligent through digital literacy education. Kaiser spoke to her own professional experience, where she witnessed firsthand the buying and selling of data to compile advanced predictive analytics. The lack of ethical and moral rules allows for manipulating the analytics in a myriad of ways, such as giving political candidates decisive campaign advantages.

She further discussed whether digital rights are human rights; further, personal data should be treated as private property and given explicit legal protections as such. If people can monetize their own data, on their own accord, their data has the potential to improve their socioeconomic status, regardless of their income level. Kaiser clarified that there should be some degree of anonymity in data aggregation, not that every detail about a person should be kept private.

For Kaiser, the future of data protection is not bleak. It’s promising. The more information the world produces, the faster some of the world’s most significant conflicts will be solved. From traffic accidents to mass shootings, the ability to secure data privately, anonymously, and securely will help prevent

wars and crises. Kaiser concluded by citing Dr. Stephen Hawking’s prediction that “technology will allow us to live in luxurious leisure.” While the future regarding private data may not be certain, technology should be built on and engaged with to have the capacity to improve livelihood across the globe.



PANEL

Manipulating Knowledge

Nina Jankowicz

Disinformation Fellow, Wilson Center

Brendan Nyhan

Professor of Government, Dartmouth College

Richard Ovenden

*Librarian, Bodleian Libraries, University of Oxford;
Author*

Moderator: Melissa Fleming

*Under-Secretary General for Global Communications,
United Nations*

The rising dominance of social media as a source of information has created a climate where misinformation plagues citizens globally with disinformation. The United Nations (UN) Secretary-General has called this large-scale disinformation and the undermining of scientific facts an “existential risk to humanity.” Climate change, war, and the fallout from COVID-19 are all global crises the world faces. The disinformation circulated online makes the severity of these threats worse as it has led to mistrust in science and institutions such as the UN. A distorted sense of history, the dehumanization of people, and in some cases, genocide, have all been products of misinformation.

This panel began with a discussion on the role that media plays in producing misinformation. Melissa Fleming explained that the current media landscape is polluted, resulting in a complete erosion of public trust. Additionally, she explained the considerable lack of investment in monitoring, flagging, and de-platforming in languages other than English. Nina Jankowicz considered the effects of disinformation on foreign policy, domestic policy, and national security. She

advocated for media detection and analysis to identify and mitigate disinformation for companies, campaigns, and governments. Jankowicz highlighted the gendered and racial aspects of misinformation and asserted that it had kept women out of the public sphere. Women of marginalized or intersectional backgrounds are more likely to encounter this type of discrimination.

Brendan Nyhan highlighted the difference between misinformation that is inevitable in a free society and misinformation that threatens the stability of our political and social systems, such as the legitimacy of our elections or the COVID-19 health crisis. While sanctions on technology may seem like an effective approach, he believes they are not warranted. Social media did not cause the phenomenon of misinformation, and therefore the imposition of sanctions is not a well-justified approach when thinking about misinformation. The panel agreed that conventional wisdom regarding social media should be questioned.

Richard Ovenden offered a different perspective to the panel. He spoke of the challenges faced in an increasingly digital world and the social importance of archives. While knowledge was once preserved in old memory institutions, there has been a shift to the online sphere. Libraries and archives are burdened with the task of maintaining the analog past, which is both technically complex and presents a financial challenge. Ovenden proposed a memory tax on private big tech companies. This mechanism would ease the conservation of the analog past and fund libraries and archives to adequately face the financial challenge of preserving the digital present.



FLASH TALK

Misinformation: Why Is It a Problem?

Lisa Fazio

Associate Professor of Psychology and Human Development, Vanderbilt University

Our brains are amazing computational machines that can comprehend complex visual scenes in milliseconds, yet they have troubling tendencies to absorb misinformation. What can companies do to prevent this knowledge neglect and encourage additional processing?

Lisa Fazio began her talk by asking the audience a simple question: “How many animals of each kind did Moses take on the ark?” Eighty percent of people who answered this question responded with the answer “two.” Revealing that it was actually Noah and not Moses who took the animals on the ark, Fazio used this exercise to show one way in which knowledge neglect operates, even when individuals knew the answer to the question.

Knowledge neglect occurs when there is a failure to use relevant knowledge appropriately in a situation. Over 30 years of research suggests that when individuals judge the truth of a statement, they rely on prior knowledge.

Another area in which knowledge neglect occurs is when individuals are given fictional stories and asked to interact with them. Fazio explained that often fiction is introduced and taken at face value, born with specific facts or ideas to make the story more entertaining. To understand how these falsehoods are constructed, Fazio conducted studies in which participants were given a piece of fiction to read, followed by a general knowledge trivia test. Fazio asserted that prior to the exercise, participants were reminded that they were reading fiction. When factual information was present in the fictional story, participants were more likely to answer correctly. Individuals who read false information scored lower on the assessment and were less likely to recall relevant and previous knowledge. Even the participants who had prior knowledge of which facts were correct or incorrect picked up false facts that contradicted what they knew.

The last example of knowledge neglect that Fazio spoke of was the effect of repetition on belief. Challenging one of Franklin Roosevelt’s claims that “repetition does not transform a lie into the truth,” Fazio asserted that while repetition cannot change the actual validity of a statement, it can change people’s perception and thoughts about a statement.

How can we get people to use prior knowledge when they are evaluating information? According to Fazio’s research, the most effective solution was to encourage individuals to actively think about their prior knowledge and the accuracy of statements being processed. Companies could foster this type of active

processing by adding features that enable thoughtful engagement with content. Fazio concluded her talk with a gentle reminder that we should think actively about what information our brains use and ingest in order to limit the spread of misinformation.



PANEL

Impact of Social Media on Global Affairs

Michelle Ciulla Lipkin

Executive Director, National Association for Media Literacy Education

Nathaniel Gleicher

Head of Cybersecurity Policy, Facebook

Shelby Grossman

Research Scholar, Stanford Internet Observatory

Moderator: Kurt Wagner

Technology Reporter, Bloomberg News

There has been a fundamental awakening to the power of social media. It is an entity that is rapidly changing and reshaping human communication. Panelists reflected on media production and consumption shifts and potential ways to increase literacy and education on a global level.

Nathaniel Gleicher discussed the positive impacts of shifting away from the original model for media production, which inhibits new voices and heterogenous discussion. However, to keep out malicious efforts on social media, a pre-review of all content may be necessary.

Social media democratizes disinformation and allows sophisticated threat actors to hide behind hired firms. Shelby Grossman provided the example of interference with the 2020 U.S. presidential election, noting that it was rooted in a Russian disinformation campaign, outsourced by an Egyptian digital marketing firm. Unfortunately, current trends show an increase in outsourcing disinformation campaigns to local actors.

Michelle Ciulla-Lipkin reminded the panel to acknowledge that skill and knowledge are limited on social media platforms. “No matter how many bad actors we take down, nothing is going to change until we fundamentally shift the way we educate our population,” she asserted. She went on to make a key distinction between technology literacy and functioning literacy.

Kurt Wagner spoke about a tweet he had posted where he tagged all three panelists, hoping that they would respond or share it. He asked the panel to distinguish a legitimate influence operation threat from his tweet and some of the difficulties faced when making determinations. Gleicher emphasized the importance of analyzing behavior and not content. He discussed a new protocol at Facebook called the “coordinated social harm protocol,” which articulates specific and narrow enforcement regimes. Grossman agreed and added that this discussion is often framed in a way that creates a stark divide between doing nothing and suspending the network. There is a range of actions platforms can take, such as down rating content and flagging certain accounts.

During the panel’s question-and-answer portion, the audience inquired about the future of social media: who should be responsible for education, when platforms should intervene, and the fake news conversation surrounding social media. All panelists agreed that platforms should partner and foster relations with civil society groups to increase media literacy and education. Gleicher added that there should be some level of collective action on platforms and that they

should be on the lookout for misleading activity. Wagner asked each panelist to offer words of advice for those interested in technology policy and social media’s impact. Finally, panelists recommended joining the U.S. Peace Corps, global engagement centers, the FBI, and looking into careers in forensic research.



FLASH TALK

Facebook Causes Protests

Leopoldo Fergusson

Professor, University of the Andes; Faculty Affiliate, The Pearson Institute

The political events that took place in the Middle East in 2011 coincided with the expansion of Facebook, Twitter, and other social media platforms. This confluence created a widespread perception that social media helped bring about the popular uprisings against authoritarian regimes. This event also reflected the now-debated importance of Facebook, the largest global social media platform, for facilitating collective action and enabling positive political change. In this context, Leopoldo Fergusson and coauthor Carlos Molina analyzed the effect of Facebook usage on political protests.

Fergusson conducted a series of studies to explore whether those with access to Facebook in their language experienced more protest and political change than those who did not. Facebook was initially launched in English in 2006 and later expanded to be available in additional languages. Tracking protest activity before and after Facebook launched a new language, Fergusson observed a resulting increase in protests by 20 percent. In an analysis of the entire span of the study (2006–16), Fergusson speculated

that there would have been approximately 15 fewer protests globally if Facebook not been available in languages other than English. However, Fergusson's research showed no evidence of any improvement in measures of governance or democracy. Additionally, Facebook expansions didn't noticeably increase the chances of regime change, quality of government, or democratic qualities. Facebook was actively used by governments, corporations, and protesters, which had individual impacts on citizens' protests. Additionally, his findings demonstrated that traditional power structures, such as political parties or traditional media, trumped Facebook's importance during critical junctures.

Fergusson claimed that measures of governments stayed the same for three different reasons. First, Facebook was actively used by both governments and influential groups to upset the effect of citizen protests. Second, traditional power structures have a more significant impact than Facebook during critical junctures. Political parties and traditional media had a more substantial effect on critical political moments. Finally, Facebook did not increase voting interest or foster amicable relationships between political parties; therefore, it was ineffective in changing other forms of political participation.

Fergusson's research did reveal one positive impact: Facebook helped decrease violent conflict. He claimed social media helps make violence more visible to the world and relevant third parties. He concluded that while Facebook does cause protests, it has been largely ineffective in producing political change.



KEYNOTE

The Future of Yemen

Tawakkol Karman

Nobel Peace Laureate; Journalist

Yemen is experiencing the worst humanitarian catastrophe the world has witnessed in decades, and the reality of the conflict has been misunderstood. “The worst manifestation of this conflict is the information and falsification of the facts,” said Tawakkol Karman. Karman provided historical context—specifically about the nature of the regime that followed the peaceful Yemeni revolution in 2011—and then described the current state of Yemen and its leadership.

Karman highlighted the nature of the regime that was ousted in the Yemen uprising in 2011 during the Arab Spring, when more than 20,000 people peacefully protested against the government. The corrupt and authoritarian regime that lasted over three decades prior to the Arab Spring brought Yemen to a state of deterioration. This display of peaceful revolution was an expression of youth and reformists who desired a more just and democratic state. The change produced a transitional process and national dialogue that defined the shape and details of the new democratic Yemeni state. Riyadh and Abu Dhabi, the counterrevolution capitals of the region,

mobilized their influence to undermine the revolutions of the Arab Spring. According to Karman, the frantic competition between Saudi Arabia and Iran provided important background on the conflict in the region. Despite conflicting viewpoints, both countries fought by proxy in Yemen and contributed to the hostility toward a democratic state. Despite its glorious ancient history, unique strategic location, and rich culture, Yemen continues to experience painful global isolation.

Karman then transitioned her discussion toward the current state of Yemen and the prospects of its future, declaring that “the Yemeni people will not surrender. We are Yemenis. We will defend our rights. We are the defenders of a just cause and will not accept the dismemberment of our country.”

Karman concluded her address by asserting the importance of ending the conflict in Yemen for the sake of regional and global peace. The security and success of international efforts must first establish the return of the state of the Republic of Yemen. The exercise of sovereignty and state institutions must be exclusively vested in maintaining democratic order. Yemenis have been ready for democracy and peace to return to their land.



CASE STUDY

Yemen in Neglect

Shadi Abu Sneida

Aid Worker, UNHCR Yemen

Juan Cole

*Richard P. Mitchell Collegiate Professor of History,
University of Michigan*

Stacey Philbrick-Yadav

*Chair, Department of Political Science,
Associate Professor of Political Science,
Hobart and William Smith Colleges*

Moderator: Afrah Nasser

Yemen Researcher, Human Rights Watch

In 2020, more than three million Yemeni people were internally displaced. In 2021, that number increased by one million and will continue to grow if drastic measures are not taken. Moderator Afrah Nasser opened the discussion by asking panelists to talk about initiatives the international community can take to address the crisis. Shadi Abu Sneida gave an overview of the crisis, reporting directly from Sana'a and sharing his experiences. He described people crowded in the streets, struggling for their next meal, and showed panelists a picture of a person holding a handful of fries, a source of food that a displaced person buys to feed his family. The funding sent to the Yemeni operation is the only source of income many Yemenis have. He described the violent frontlines, lack of health care, and absence of education, and asserted that the real solution is to call a cease-fire and restore the ports to establish peace in Yemen.

Stacey Philbrick-Yadav spoke about the representation gap between Yemen's political elites and the people engaged in the everyday struggle. Her research focuses on the dynamics of Yemen's political parties. She

claimed that the international community should treat Yemen's political parties as the primary representatives of Yemeni society. She called the parties part of the old system, noting that the protests in 2011 were not just against Ali Abdullah Saleh but also against the political parties. Ironically, these parties were the primary beneficiaries of the last postconflict settlement and are poised to benefit from any newly negotiated agreement. The bilateral framework for negotiations created by the UN Security Council Resolution 2216 requires that an agreement be sought by the Houthis and the government, which she deemed utterly unreasonable. Analysts, observers of Yemen, and Yemeni activists agree. She advocated for a more inclusive peace process to produce a more durable and sustainable outcome.

Juan Cole discussed the role of the United States in the conflict and what the administration should do to handle it. He said that the United States should be concerned with Yemen for two reasons. First, the United States is responsible to a degree for this crisis. Second, it may be the issue that reforms the relationship between Congress and the Presidency. While the Biden administration has some cursory involvement, the United States is still selling weapons to the Saudis, the same weaponry used in Yemen. Cole noted the bipartisan support for a new War Powers Act that would take power to declare war from the president, if passed. While this new measure would allow Congress to stop future wars, Cole remained apprehensive about the measure's ability to end the Yemeni conflict. Panelists also discussed the necessity of creating channels to enable Yemenis to access what

is going on at an international level. Philbrick-Yadav noted that current congressional activism is oriented toward ending U.S. complicity, and a new negotiating framework is needed.

Audience members inquired about steps needed to engage the international community moving forward. Civilians in Yemen deserve peace, and a resolution between parties in conflict is long overdue. Abu Sneida stated that "international actors should see Yemenis as they see their people." Philbrick-Yadav noted that the Yemeni conflict had not caused the migration pressures or images that other wars have produced. She further stated that she didn't know how to help it be less neglected. Panelists reiterated that the Yemeni conflict is the worst humanitarian crisis the UN has seen since WWII and needs to be prioritized. Panelists urged the audience to find Yemeni partners and write policymakers to show urgency.



FLASH TALK

Gang Rule

Chris Blattman

*Ramalee E. Pearson Professor of
Global Conflict Studies,
Harris School of Public Policy,
The University of Chicago*

Gangs govern millions worldwide. Many argue that criminal rule provides protection when states do not and that increasing state services could crowd gangs out. Chris Blattman conducted a two-year, gang-level field experiment to investigate intensifying city governance in select neighborhoods.

All states need governance. However, in Medellín, Colombia, a different option exists for the people. Known as combos, this type of staffing structure (that governance) is made up of organized neighborhood gangs that run the local drug business and provide governing services for a small fee. Every low- and middle-income neighborhood in the city has a combo responsible for some form of governance. This additional source of authority creates a duopoly between the combo and the Colombian government.

For the past six years, Blattman and his team have documented every combo, their approximate location, and how they operate. While every combo has a territory and offers some governing services, some combos provide higher levels of governance than

others. His research revealed that both actors operate in every neighborhood: the state and the combo are both governance providers. Blattman considered the following two questions: What's a city to do in these circumstances? How does the city combat them?

He speculated that with sufficient investment, the city could crowd out combo rule, forcing gangs to focus on other markets. For example, in 1987, the government of Colombia subdivided the city, creating 16 new areas called comunas. The new internal borders disrupted the way protection services were received as state service headquarters locations changed. When the government started providing better services, so did the combo.

Blattman's research revealed that when the state increased governance, the combo gained more legitimacy from citizens in the neighborhood. This makes territories with the most drugs the most valuable and desirable to govern for both the state and the combo. Blattman offered potential solutions, such as tackling underlying rents to reduce drug profits, making these territories less attractive, providing treatment to addicts, legalizing certain drugs, or reducing consumer demand. However, he noted that any solution that reduces drugs and elicits profits could lead to extractive and violent gangs.

Blattman highlighted the complexity of tackling organized crime on a global level, stating that "it's a perilous and difficult path, but it's a crucial one to walk down because it isn't just a problem facing Medellín." Hundreds of millions of people live under

some criminal rule. He emphasized the need to study and understand crime organizations to create a new approach before the problem worsens.



“We’ve also worked to bridge the gap between policy-making and the evidence that scholars produce, and The Pearson Institute is a crucial contributor to this endeavor. Since its founding, it’s been dedicated to bringing rigorous evidence to bear in conjunction with policymakers to ensure that we can bring the best tools that we have to help mitigate and resolve and prevent global conflict.”

Wednesday, October 13, 2021

Welcome

Katherine Baicker

Dean and Emmett Dedmon Professor, Harris School of Public Policy, The University of Chicago



CASE STUDY

Iran

Pouya Alimaghani

Lecturer and Historian of the Modern Middle East, Massachusetts Institute of Technology

Majid Khadduri

Professor of Middle East Studies and International Affairs, School of Advanced International Studies, Johns Hopkins University

Vali Nasr

Non-Resident Senior Fellow, Atlantic Council

Mahsa Rouhi

Research Fellow, Institute for National Strategic Studies, National Defense University

Ali Vaez

Senior Advisor to the President and Iran Project Director, International Crisis Group

Moderator: Negar Mortazavi

Journalist and Political Analyst; Host, The Iran Podcast

Panelists discussed Iran’s various foreign and regional policies, Iran’s nuclear negotiations with the United States and Europe, and the barriers both actors must overcome to achieve peace. Negar Mortazavi opened the discussion by asking panelists to comment on the recent nuclear negotiations with Iran under the Biden administration. Ali Vaez said, ironically, the state of play is in suspended animation and has been for months. Enrique Mora, the chief negotiator for the European Union, is scheduled to visit Tehran to meet with his new Iranian counterpart, Deputy Foreign Minister Ali Bagheri, to discuss the future of Iranian negotiations, or Iran’s willingness to negotiate. Panelists discussed measures Iran must take, including closing unresolved discussions from the Rouhani administration, cooperating with IAEA (International Atomic Energy Agency), giving access to global inspectors, and transparency on Iranian nuclear activities.

Even if Iranians cooperate with the agency, negotiating will be a complex process due to the strained relationship between the United States and Iran. Vaez generalized these pressure points in four

different ways. First, there has been Iranian pushback against keeping sanctions imposed during the Trump administration, a measure the current administration has not taken. Second, the West expects Iran to take nuclear measures, in an effort to replicate the nonproliferation threshold that the failure of the Joint Comprehensive Plan of Action (JCPOA) put in place. Third, Iran demands guarantees that the United States won’t undermine sanction relief in the future, ensuring the long-term survival of JCPOA. Finally, the United States demands that Iran commit to continuing negotiations once the JCPOA is restored. To overcome these hurdles, both sides must be flexible and revise their redlines or risk war. If the United States does not provide verification mechanisms to Iran, it could lead to an escalation cycle between Iran and the United States.

Mortazavi shifted the conversation toward foreign policy in Iran and the economic, political, and diplomatic shift from the United States toward China and Russia. Previously, under Rouhani’s rule, Iran’s foreign policy favored a nuclear deal, an attempt to anchor relations with the East. Historically, Iran has looked to the West and United States; even its constitution was predominantly French and Belgian. China and Iran relations are not new but have become much more intense, as China keeps Iran’s economy afloat through manufacturing deals and purchasing oil. Nasr claimed the failure of JCPOA ended the idea that Iran could be equidistant between the East and the West, thereby having an adverse effect by making Iran more reliant on the United States. Mortazavi added that the future of negotiations with Iran relies heavily on the incentives Russia and China may provide. The

result is a dichotomy between the government looking to the East while large population segments consume Western culture.

The audience inquired about international aid extended to the Iranian people through a humanitarian framework if the JCPOA talks fail. Panelists speculated that if there is no prospect of reviving JCPOA, Iran would be highly unlikely to engage in any transactions. Panelists also discussed how current sanctions affect these dynamics. Alimaghani noted that when COVID-19 hit Iran, the United States did not provide temporary humanitarian relief, despite Iran being the epicenter of the virus in the Middle East. The relationship was further strained when the Trump administration used COVID-19 to tighten sanctions during Iran’s weak moment.

Panelists discussed the future of Iranian relations with the United States and voiced concerns for the future. The current regime is shifting domestic policies toward securitization and conservative consolidation. Iran faces the possibility of succession without the social and economic stability to overcome one; infrastructure degradation has already caused water, electricity, and energy shortages due to a lack of investment. While Iran faces an uncertain future, policy issues cannot be resolved if suspended outside their political context.



FLASH TALK

Russia's Firehose of Falsehoods

Konstantin Sonin

*John Dewey Distinguished Service Professor,
Harris School of Public Policy; Faculty Affiliate,
The Pearson Institute, The University of Chicago*

Russia has been perceived worldwide as a source of misinformation and propaganda. However, the ways these campaigns operate and form have not been accurately portrayed. Konstantin Sonin highlighted different points about Russia's disinformation campaigns that have been overlooked and provided an overview of Russia's information operations.

Russia's disinformation campaigns are far less sophisticated than what is typically described. While the investigation carried out by special prosecutor, Robert Muller, resulted in several indictments, the sums of money that the Russian government allegedly spent on social media campaigns were strikingly low. Sonin pointed out that the same amount is spent weekly by a presidential campaign in the United States.

Misinformation campaigns in Russia are far less consequential than perceived. For five years, researchers in economics, political science, and computer science have worked with the data related to the 2016 U.S. presidential campaign, yet have failed

to produce any evidence that information campaigns had or have any impact on people's votes.

Sonin made a more general point that while information operations make for a fascinating discussion, they are not impactful. Sonin discussed the presidential election in Belarus in 2020. Despite having all the media at his disposal and putting his political opponents in jail, Alexander Lukashenko still had a large margin of Belarusians vote against him. Lukashenko is still in power, suggesting that the actual use of force is much more impactful than informational campaigns and propaganda. The same principle occurs in Russia, where information campaigns are received one hundred times more than in the United States. These campaigns are not impactful when the fundamental mechanisms at play are the prospect of jail, exile, and in extreme cases, execution.

Sonin concluded by asserting that Russians believe that the same type of election and political corruption occurs in the United States. The idea that elections are stolen and that political corruption occurs is a reflection of what Russians believe is true of their own elections. Russian propaganda is a reflection of the Russian leader's beliefs and not a specific attack on the American people.



CASE STUDY

Saudi Arabia

Gregory F. Gause

*Department Head and Professor,
Bush School of Government and Public Service,
Texas A&M University*

Adel Hamaizia

*Associate Fellow, Middle East and North Africa
Programme, Chatham House*

Karen House

Senior Fellow, Belfer Center, Harvard University

Pascal Menoret

*Renée and Lester Crown Professor of Modern Middle
East Studies, Department of Anthropology,
Brandeis University*

Moderator: Arwa Damon

International Correspondent, CNN

The panel opened with a discussion of regional and international dynamics as the contradiction between Saudi Arabia's external image and reality. Gregory Gause described the Saudi regime as "Draconian," as it inhibits political openings that cause social reform. The bulk of the private sector in Saudi Arabia has been centered on cheap energy and labor, which creates a severe problem for the country. Pascal Menoret noted that Saudi Arabia has massive production capabilities, giving the Kingdom the power to postpone broader conversations about the environment and continue contributing to global dependency on fossil fuels.

Menoret stated that Saudi Arabia's power is reflected through their recent efforts to stop UN experts from reporting the war crimes in Yemen. He expressed his concern for the militarization of politics and policy worldwide and the military-industrial complex.

Karen House discussed external and internal efforts by the Kingdom's government to spread misinformation. Externally, Saudi Arabia has become more active and it is speculated that this is done intentionally to distract

people from domestic issues. Internally, they are covering their activities in Yemen and manipulating the message.

Adel Hamaizia expanded on this conflict, highlighting the fact that the Saudis have a better strategy for managing the information field internally than they have had in the past. The government's plan for information management, paying trolls to flood the Twitter sphere to drive progovernment conversation, has been more effective in distracting political speech in the public sphere than old strategies.

Audience members inquired about the relationship between Saudi Arabia and Israel and driving interest in the countries. While the crown prince would welcome an open relationship with Israel, both for his regional ambitions for foreign domestic investment, and a shared belief that Iran is a perceived regional threat, the king is not interested in fostering relations with Israel. While an open relationship with Israel may decrease criticism in Washington, Gause noted this is unlikely while the king is still alive.

Panelists concluded by discussing the direction Saudi Arabia is headed and what they hope to see. Despite the millions of dollars the Saudis spend on public relations campaigns, or the billions of dollars spent on weapons, they cannot control the information space in the United States. Hamaizia noted that a political opening that allows for criticism and healthy feedback is imperative to addressing issues on the economic front. Menoret concluded the panel by asserting that there are "a lot of global similarities when we're talking

about broader politics," arguing, essentially, that Saudi and American people want many of the same things.



FLASH TALK

Comparative Constitutionalism: Islam in Perspective

James A. Robinson

*Institute Director, The Pearson Institute;
Reverend Dr. Richard L. Pearson Professor
of Global Conflict Studies and University Professor,
Harris School of Public Policy and
Department of Political Science,
The University of Chicago*

Why is it that different societies today and in history write such different constitutions? Twenty years ago, after the Western powers invaded Afghanistan, the German city of Bonn hosted a conference to re-create the state of Afghanistan. The meeting initiated a constitutional process that eventually led to the 2004 Afghan constitution. Now the Taliban are back in power, and there is enormous speculation over what kind of constitution the Taliban will write and how the state will be organized.

In this context, James Robinson presented a comparative constitutionalism study. He claimed that the 2004 Afghan constitution was a liberal democratic constitution. To engage within this context, Robinson provided an overview of the standard features of Western constitutions. He asserted that Western political philosophy has been highly concerned that rulers will behave unlawfully. Aristotle famously proposed the notion of spreading power between groups as a solution to tyranny. This notion was a clear progenitor for the development of separation of powers solidified in the U.S. constitution. Robinson

asserted that these traditions come from personal history, and political ideas reflect history as well.

Robinson made the point that Islamic constitutional history departs from traditional theory. Neither Muhammad nor the Four Caliphs were ever subjected to institutionalized checks and balances. The Islamic tradition is not concerned with the type of misbehavior of rulers that dominates Western theory. The concept of legislation in Islamic tradition is irrelevant as God created the sharia and the laws. The system of the West is complex, with many ideas and interests at play, which creates uncertainty in rulers. In contrast, the implementation of sharia is a ruler's duty, simplifying the matter. Additionally, Robinson highlighted that the people of Islam need to collaborate and discipline rulers more efficiently than what we see happening in the West.

He concluded by speculating that the new constitution will not be liberal democratic and resemble the 2004 Afghan constitution. Political institutions are not needed because sharia shapes all laws and policies. To understand the kind of constitution the Taliban will have, Islamic history and culture must be understood. However, "if we want to influence the policies and institutions of the Taliban in a direction that we feel is consistent with these universal principles, then we have to understand the rationale for these institutions and entry points where we might engage with them on the grounds that make sense within their tradition."



“The University is deeply committed to fostering free and open dialogue, which allows for the unfettered exchange of ideas and compels us to examine our assumptions and open the door to innovation.”

Thursday, October 14, 2021

Welcome

Ka Yee C. Lee

Provost and David Lee Shillinglaw Distinguished Service Professor, Department of Chemistry, James Franck Institute, Institute for Biophysical Dynamics, and the College, The University of Chicago



KEYNOTE

Constant Confusion: Technology Meets Modern Conflict

Brett Goldstein

*Former Director, Defense Digital Service,
U.S. Department of Defense; Pearson Associate*

Brett Goldstein began this address by highlighting his background in the private sector, including his role as the former Director of the Defense Digital Service at the U.S. Department of Defense. He described the Defense Digital Service as a tier-one technical unit, a “SWAT team of nerds.” He noted that through his role there he addressed issues like the COVID-19 outbreak on a naval carrier, and learned a great deal about the influence of cybersecurity on modern conflict.

Goldstein said we are stuck in history with conventional thinking that has developed into how we think about national security. The nuclear triad has brought stability to topics that are inherently intimidating. In contrast, it is not so simple to grasp when we look at cyber issues and track how electrons travel with a highly minimal footprint or trail.

The first topic Goldstein discussed was attribution through conventional modalities, mainly kinetic modalities. The Boston marathon bombing was a kinetic bomb attack that could be studied and investigated through biology, kinetics, and nuclear science. These

topics are well understood in academia. Cyberattacks, on the other hand, have much more anonymity.

While science breaks down how to track a missile, cyberattacks cannot be traced to just one place or person. Goldstein broke down his thought process by using a visual of a hack attack from New Zealand. While he can see that the source was from New Zealand, he still must ask, “Is it really coming from there?” Traffic online has very little meaning in cybertracing, unlike tracking a missile. By simply using a VPN, traffic can be sourced across the globe despite the real location. In the case of an attacker trying to add further anonymity, they could do multiple “hops” to send attacks through several different places before landing on the intended destination. Goldstein reflected on the 2021 Colonial Pipeline ransomware attack, in which the Texas-based pipeline company was attacked. The perpetrator filtered the cyberattack through multiple, varied sources in order to conceal the origin of the attack, which confused investigators and made it difficult to determine the true source of the attack. Attackers can perform malicious acts and hide attribution at low cost—such is the nature of modern conflict.

Deep thoughts—a function of artificial intelligence that can take a person’s emotions and simulate physical actions—are another complex use of modern conflict. He demonstrated this through a video of former U.S. president Barack Obama discussing inappropriate topics (that is, inappropriate given his position). At the end of the video, it is revealed that it was comedian Jordan Peele doing a convincing impersonation of

Obama’s voice, utilizing deep thoughts to make it appear as if Obama was saying Peel’s words. Goldstein further discusses how threatening this technology is because it has the capacity to be carried out in real time to promote public misinformation or worse. This can also be further carried out through Twitter, in which public opinion can sway reality to create an entirely new narrative that is completely divorced from reality.

Goldstein notes that there is a lack of information and research about understanding conflict and cyber effects. Goldstein observes that “academia needs to make more of a contribution,” especially when considering how rapidly cyberattacks are carried out.



PANEL

Artificial Intelligence and International Security

Gregory C. Allen
Director of Strategy and Policy, Joint Artificial Intelligence Center, U.S. Department of Defense

Raluca Csernatoni
Visiting Scholar, Carnegie Europe

Kara Frederick
Research Fellow, Technology Policy, The Heritage Foundation

Herbert Lin
Senior Research Scholar, Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security, Hoover Institution, Stanford University

Moderator: Matthew Rosenberg
Correspondent, The New York Times

Matthew Rosenberg opened the panel by commenting on Nicholas Chalan, who quit his job as Chief Software Officer for the U.S. Department of Defense. Chalan believed that the United States was falling behind China in the technology race in ways too difficult to overcome. Rosenberg speculated that this was not a uniform view at the Pentagon and asked panelists if Chalan’s claims had any merit.

Gregory Allen pointed out that Chalan had come out with a statement clarifying his remarks (he claimed that he had been misquoted). The correct interpretation of what he said is that the United States is at risk of losing its technological supremacy. Allen made the point that the U.S. military has grown accustomed to operating in largely uncontested environments over several decades. He said that leadership at the most senior levels of the EU, Russia, and China all agree on one significant point: “Artificial intelligence is going to be foundational to the future of competitive military advantage in terms of technology.”

China’s most recent defense white paper, the equivalent to a national defense strategy, identified artificial intelligence technology underpinning a military technology revolution. Rosenberg mentioned how China and powers worldwide have a full-on rush approach into AI, automating weapons, and cyber defense systems. Herbert Lin expressed skepticism of this approach as well as concern about the United States going on the record saying it will not neglect ethical and safety issues when it comes to the deployment of AI. Paying attention to these issues is an inherent slowdown of the pace with which we can develop technologies and integrate them into military systems.

Although it is tempting to prioritize weapons and technology, Lin advocated for the military to also invest in artificial intelligence to improve interoperability between Department of Defense systems. The military is a substantial administrative organization, and this operational component should not be neglected. According to Lin, AI could improve databases, human resources, payroll, and other administrative pain points.

Rosenberg turned the discussion toward the European approach to disruptive technology. Despite the United States’ position as a militarist power, the European Union is far ahead in emerging technologies. Raluca Csernatoni attributed this to Europe operating more strategically than the United States in the nexus between technology and security. She gave the example of the strategic compass process, a process in Europe where member-states are involved in thinking more geopolitically about a threat

assessment landscape, a step that the United States is not yet prepared to take. Finally, Kara Frederick considered the implications of having an authoritarian government like China make strides in interoperability before the United States, which would allow them to draw value from data that could identify anomalies against competitive nations. She considered the legal atmosphere in China and noted that their national intelligence laws provide another layer of leniency.

Rosenberg highlighted how we no longer need governments to produce weapons. Despite having a weak handle on Python and XML code, if he were given an Amazon account or a credit card, even he could develop a weapon. He asked the panel if there was a sure way to think about conceptual roadblocks such as procurement. Panelists discussed the need to reconceptualize what the world will look like in a broader sense, as current trends project more than five billion people will have internet access by 2025.

Panelists also discussed national security and geopolitical implications of an increasingly digital world. Lin expressed the need to take risks and take more significant steps to integrate systems in the United States. Participants agreed that the United States will take appropriate technical and procedural safeguards to minimize risk. Allen commented on the stakes: “We play in an area where life-and-death stakes are operating safety-critical technologies involved in the use of force. This is an astonishingly difficult task.”

Audience members inquired about ways to leverage AI to further collaborative space exploration research,

and the competitive situation with adversaries. Panelists agreed that space exploration is a driver for technological innovations but expressed the need for an international governance regime or space traffic management. Indeed, democratic values and human rights are at the forefront of developing these technologies and their use for security and defense purposes.



FIRESIDE CHAT

AI, War, and National Security

August Cole

*Author; Non-Resident Fellow,
Brute Krulak Center for Innovation and Creativity,
Marine Corps University; Non-Resident Senior Fellow,
Scowcroft Center on Strategy and Security,
Atlantic Council*

Moderator: Vivian Salama

National Security Reporter, The Wall Street Journal

“Data is the new ammunition,” opened August Cole, as he described the large-scale implications of increasingly capable computer power. Artificial intelligence can both target a missile with pinpoint accuracy, and perhaps more troubling, fundamentally influence human behavior. The level of data used by advertisers on social media platforms is precision that psychological operations professionals can’t imagine, a precision that shapes emotional triggers. Algorithms are composed of the data accumulated from online behavior, behavior that reveals what a person does and how they feel about it.

For example, the technologization of communication and disinformation could allow wars to be waged without seizing territory or military presence, a domain of warfare that military organizations are not equipped to handle. Therefore, Cole posits, a fundamental reassessment of military and defense spending is required, incorporating disinformation specialists and collective military acknowledgment of AI warfare. These technologies will cause profound societal changes that are often overlooked by AI robots.

Cole considered the future of these technologies, evolving to capabilities that could affect confidence in systems of government. Vivian Salama inquired about China's transformation from land forces to intelligent warfare, a technological stride the United States has not made. While Cole does not disregard the wealth China will accumulate through a civilian and commercial AI sector, he hopes that China's focus on AI serves as a reminder that the United States must make efforts to advance and explore creative channels. China and Russia can wield enormous amounts of computing power, entering the cognitive warfare framework. While Chinese President Xi Jinping is advocating for a 20 billion dollar investment in AI, the willingness to experiment with the government and invest more in technology is lacking in the United States. In his recent research, Cole found massive gaps that make the United States vulnerable to the conventional internet as we know it, indicating that the current defense framework needs to adapt.

Salama concluded the talk by asking Cole to reflect on his works of fiction as a tool to approach security issues. To Cole, fiction allows a type of storytelling to make different points of view and positions more accessible: "We are trying to allow people to be able to inhabit future worlds that don't exist so they can be better prepared for them, and ultimately that is one of the oldest storytelling technologies of all."



FLASH TALK

Trends and Insights from the Ransomware Ecosystem

Jeff Moss

Founder and Director, Black Hat and DEF CON

In 2010, Intel released an updated CPU (Central Processing Unit) that included encryption capabilities, allowing computers to operate encryption at a noticeably higher speed. When digital currencies hit the market, promising privacy and anonymity, it enabled the financial underpinnings for modern ransomware attacks, both from organized crime and nation states. Jeff Moss asserts that paying the ransom is counterintuitive, as nothing with these ransomware groups is guaranteed: "Just because you pay them, just because they tell you they've deleted your data, they haven't. There's no guarantee that another group doesn't come along and steal that data right out from underneath the other criminal." In other words, they could still sell the data to a government or competitors and leak data to the media while continuing to profit from it.

The second type of ransomware Moss presented is operated by a nation-state and not considered organized crime. According to Moss, nation-states have different motivations and can work with organized criminals or offer protection to

organizations that elicit illegal activity. He claimed that there would be no legal cooperation in the United States, even if the foreign nation is identified, because these situations are out of the norm. Even if the individual is not adjacent to the government's issue, anyone can be randomly targeted and become collateral damage. Moss then discussed a scenario that could occur if a targeted individual decided to make the payment. The more people pay ransoms, the more competition, innovation, and money are given to organized criminals.

Moss believes this will continue to progress, and it will get increasingly more difficult for law enforcement to track. Paying ransom will inevitably lead to a permanent interest of a class of companies that benefit from the existence of ransomware. Moss discussed the tools needed from legal departments and how criminals and nation-states must be treated as a two-pronged problem.

Moss concluded by encouraging governments to carefully consider and investigate regulating and making ransom payments illegal. The future could be bleak, but Moss believes that if consumers collectively ignore ransom demands it might put an end to the trend. Moss encouraged the audience to reinstall and upgrade their systems to avoid preemptive ransomware attacks.



PANEL

Cyber Abuse, Security, and Defense

Deborah Housen-Couriel

*Chief Legal Officer and VP Regulation, Konfidis Ltd.;
Advisory Board and Adjunct Professor, Federmann
Cyber Security Center, Hebrew University of Jerusalem*

Christopher Painter

*President, The Global Forum on Cyber Expertise
Foundation; Former Senior Director for Cyber Policy
and Acting Cyber Coordinator,
U.S. National Security Council*

Philip Stupak

*Senior Advisor, Management Directorate,
Office of the Chief Information Officer,
U.S. Department of Homeland Security;
Lecturer, Graham School, The University of Chicago*

Moderator: Ellen Nakashima

National Security Reporter, The Washington Post

Ellen Nakashima opened the panel by putting the threat of cyberabuse into perspective. For the past two decades, there's been a lot of rhetoric about a cyber-war when, in fact, no such thing has happened. The world is more digitally connected than ever, and the ability to penetrate closed computer systems and disrupt physical processes has created a wealth of capabilities. These capabilities can be harnessed to malign ends, meaning that cyber does not always cause conflict; instead, it is a tool used by states to advance their geopolitical agendas. Nakashima asked panelists to provide insight into which cyberthreats should receive the most attention as well as why it is espionage to steal political secrets from the United States and other countries.

Chris Painter talked about common misconceptions about cyberthreats and asserted that they are a mainstream national security issue within a larger geopolitical landscape. He explained that espionage is not a disruptive activity: "Espionage has happened since the beginning of time, and it will happen until the end of time." Painter said that ransomware is the

real security issue, as it interferes with business and government continuity and has a discernible natural effect. He voiced his worries about the integrity attack, which makes data unreliable.

Deborah Housen-Couriel advocated for critical infrastructure analysis to understand vulnerabilities that will present themselves in the future. Another factor she considered was the role of global dependencies, such where national electrical systems connect and interlock with other countries.

Nakashima informed the panel that the Biden administration had just released a joint statement acknowledging ransomware as a threat to security and the economy. She asked Phil Stupak what he thought the prospects were for this approach. He voiced the importance of having like-minded nations recognize that ransomware is a common scourge: “[President Biden doesn’t] believe that we’ve had a moment like this within cybersecurity.” Christopher Painter called it a significant achievement, despite the commitments not being concrete.

Panelists discussed whether they supported the use of the military to disrupt ransomware networks. Housen-Couriel and Painter agreed that military action should be at least considered as a tool. Painter said he had reservations about using the military to go after adversary infrastructures in third-party countries and noted that a collective response might be more productive. The more significant problem is that while there may be disruptive value in going against a ransomware group, they will regenerate. Stupak said

he had grave concerns about using the military combat ransomware. He highlighted the lack of sovereignty within cybersecurity and discouraged militaries from acting beyond their borders to combat ransomware.

Panelists answered questions about cyberdeterrence, private-sector security, and Israel’s cyberdefense. While private companies hold 90 percent of critical infrastructure in the United States, Housen-Couriel explained that this is not the case in Israel. She pointed out its small professional cyber community trained by the Israeli army, allowing it to make changes quickly and implementing several national programs that taught students in cybersecurity education. All panelists agreed that the time has come for some minimum standards for critical infrastructure.

FLASH TALK

The Quantum Revolution: A New Paradigm for Communication

David Awschalom

Liew Family Professor of Molecular Engineering and Vice Dean for Research, Pritzker School of Molecular Engineering, The University of Chicago



David Awschalom began his address by noting memorable events that happened in 1969: The Beatles’ last public performance, the first man landed on the moon, and the first ARPA (Advanced Research Project Agency) project to successfully link two processing systems, marking the first step of developing quantum technologies. Today, quantum technologies offer new capabilities across sectors.

Awschalom discussed that even though technology got physically smaller as devices approached the atomic scale, quantum properties emerged and developed for radically new applications. “While we’re living in uncertain times today, uncertainty is a basic property of quantum systems,” Awschalom asserted. He explained that information is either a zero or a one, while a quantum bit is a combination of both. This property, superposition, expanded the computing and global communication capabilities of quantum technologies. Another property Awschalom discussed was entanglement, a uniquely quantum way to connect quantum bits. Current encryption schemes for banks and governments are safeguarded by using

large numbers and their prime factorization. Awschalom asked the audience to imagine the arrival of a quantum computer that could solve this quickly and to think about the dramatic implications for cyber security.

Awschalom anticipates quantum communication will also impact governments and multinational companies. Already, more than 20 million dollars has been allocated to government programs launching quantum initiatives. He applauded these initiatives and was encouraged to see technology development on a global level. However, governments are not the only investors, and large-scale industries and financial companies have begun industrial engagement. These investors are raising questions about the quantum supply chain for materials, and Awschalom reminded the audience that this was only a snapshot of the rapidly growing global industrial engagement. According to Awschalom, quantum technologies have the potential to create a diverse and equitable workforce. Successful quantum technologies will require skilled workers and implementation of technical programs and training initiatives.

Awschalom concluded by highlighting the opportunity that quantum technology development creates in addition to balancing privacy and innovation. It is a moment to think about a new way to build a diverse and inclusive work source. "It's an opportunity for all of us to work together and try and resolve these issues because the most exciting impacts in this field have yet to come."

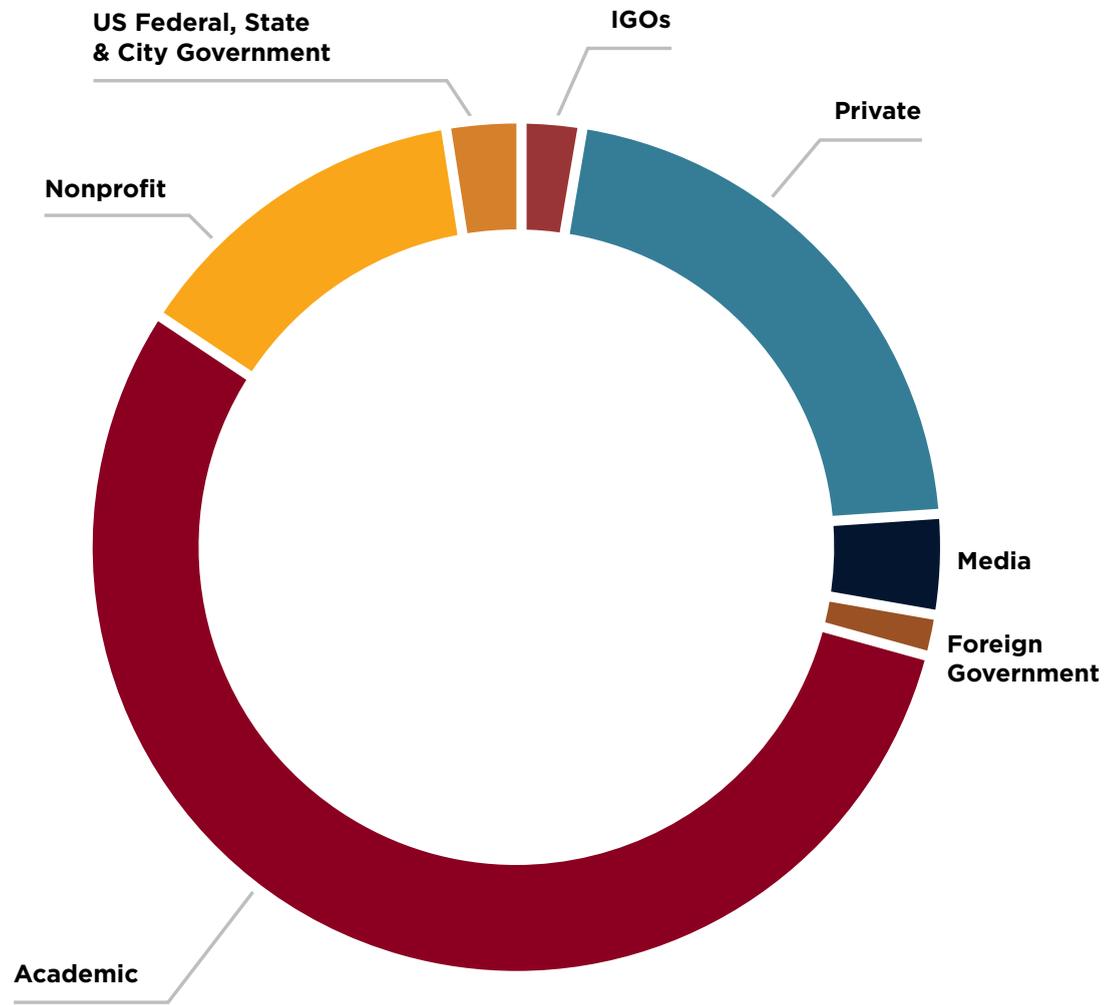


Participation Infographics

Geographic Participation



Sectors Engaged



Background text: ADE3100A16C20Data BreachE204865216E6420746
08 2202E6F6163686573204C697474CC 520
0BA01Cyber Attack696EA1 86FAF6420
4023 106564207368 06E61C F766 6C79
627 C6E207468652AA261736B60142E204
C010046868AF93010808B4FA017745C7A6 108
0F00FAFA33C08E00F2A5697D011A56AFE64
F1D01 02073 C732C20736852756B013 0AA2
6AD8 616E64200171719System Safety Com
00E2A5694C028BE5BF7D011A001CA3E

0046868AF

93010808B4FA017745C7A6

01

02073