International Symposium on Sustainable Development: Cybersecurity

Indiana University—Kelley School of Business—Friday, January 26, 2018

An official synopsis of the day written by Justice O. Eiden

Objective: To provide attendees with insight amongst a variety of different concepts where the practice of cybersecurity and sustainability can merge to create sound and sustainable policies for current and future technologies.

The event began with an opening speech from Dr. Scott Shackelford, an Assistant Professor at the Kelley School of Business and the Director of the Program on Cybersecurity and Internet Governance at the Ostrom Workshop. In his short introduction, he provided attendees with a roadmap of themes that would be addressed during the day and policy implications for our technological age. Dr. Shackelford provided the objective for attendees and participants to address possible analogies between sustainable development in the economy, the environment, and in cybersecurity and how working to create sustainability in one area means that all others need to be addressed.

Next, Liisa Past, Chief Information Officer at the Estonian Information Authority, provided attendees with the symposium's keynote address. In her remarks, she described the vitality of cybersecurity as it is need to "protect a way of life" for people, across cultures and nations throughout the world. Absence of security that is regulated by both national and international governments and the private industry (who creates the hardware and software that makes cyber possible) would throw the individual's confidentiality and the accessibility of their own information into flux. Additionally, she warned that failure to buttress existing cybersecurity practices as well as to create new and more sustainable ones could lead to information asymmetries between nations, which could lead to unnecessary conflict and war. She closed her remarks by urging attendees to realize that nation-states, of all ideologies and governance structures, need to work together in the field of cybersecurity to create international legal norms to lower the risks of conflict vis-a-vis nation states.

First Panel Discussion -- Sustainable Cybersecurity: A Global Perspective

Indiana University Kelley School of Business professor Dr. Scott Shackelford moderated the first panel discussion. Shackelford noted that there are important lessons to be drawn from sustainability efforts in the global economy and environment that could be applied to the field of cybersecurity.

Megan Stifel: Founder & CEO, Silicon Harbor Consultants, LLC: Stifel began her remarks by looking to the future of the proliferation of web-based content and technologies into our everyday lives. She claimed that government and the private industry need to further adopt sustainability standards that safeguards consumer's private information. She further argued that for this sea change to take place, the private industry needs to create "...a consumer-based

understanding [of cybersecurity and cyber threats] ...by developing a lexicon for consumers to understand encryption and cyber safety."

Brian E. Ray -- Professor of Law, Cleveland State University: Dr. Ray began his remarks by stating his skepticism with drawing analogies between cybersecurity and sustainable development. He reminded the audience that while attempting to discover parallels between the development of these two broad concepts can fuel discussion in the field of cybersecurity, some attempted analogies are not necessarily useful in this particular context. Additionally, he discussed the differences between China and the U.S. with their views on cybersecurity as it related to sovereign governments seeking to gain advantages or cause damage and destruction vis-a-vis their adversary. Lastly, Dr. Ray concluded that this issue, due to different conceptualizations of development, freedom, and security between nation-states makes regulating cybersecurity a difficult venture, albeit a necessary one.

Marios Efthymiopoulos -- Associate Professor of International Security & Strategy, American University in the Emirates: Dr. Efthymiopoulos concluded the panel's opening remarks by providing international insight in the field of cybersecurity. He went to great lengths to describe how his home nation, the United Arab Emirates (UAE) deals with the issue of cybersecurity as an emerging nation in the Middle East. He claimed that cybersecurity not only is beneficial for sustainable development in emerging nations, but also, necessary to ensure that nation's vital infrastructure and the personal information of its citizens is safeguarded.

Second Panel Discussion -- Freedom v. Security: Is there a Sustainable Balance?

Professor Joseph A. Tomain of Indiana University's Maurer School of Law opened the panel by briefly touching upon the historical tension between freedom and security. He then asked the panel to address this particular question in their opening remarks, "…does 'cyber' change the freedom vs. security question?"

Jolyon Ford -- Associate Professor: Australian National University: Dr. Ford opened the panel posing the question to himself and to the other panelists of whether or not the incorporation of the aspect and reality of "cyber" into the freedom vs. security debate changes its dynamics. He then dove further into the semantics of "security" as he sought to define security in different contexts in different nations. Developing nations usually view security only as it applies to the states, while developed nations usually look to promote both state and human security, he said. Dr. Ford closed his remarks by stating that to create sustainable cybersecurity, especially in developing nations, the private industry, meaning the developers and suppliers of technological hardware and software, need to be incentivized in some fashion to create sustainable development outcomes.

Jaclyn Kerr -- Research Fellow, Center for Global Security Research, Lawrence Livermore National Laboratory: Jaclyn Kerr opened her remarks by asking what is it that we're trying to sustain with cybersecurity. Is there a one-size-fits-all approach for cybersecurity? Are nations

more invested in sustaining security or democracy with the utilization of cybersecurity? All of these questions have no easy answer as each nation deals with this issue in a different fashion. The second part of her opening remarks were devoted to the proliferation of fake news and its relation to the freedom vs. security debate. According to Kerr, foreign nations have more power than even in human history to influence the media of another nation thanks to social media and other digital platforms. She concluded by stating that issues like fake news and misinformation will cause more governments to impede on the democratic elements of digital social spaces in return for security.

Wafaa Mamilli -- Vice President, Chief Information Security Officer, Eli Lilly & Company: Lastly, Wafaa Mamilli provided the perspective of private industry in the freedom vs. security debate. She stated that the primary goal of the Eli Lilly corporation's cybersecurity infrastructure is to safeguard its patents, medical information, and research. Eli Lilly, as a private company, prioritizes security over freedom due to the high stakes of having information stolen or used in a negative way against the public. In this realm, as Mamilli stated, there's also issues with information being stolen which may lead to huge financial loss for the company. In conclusion, Mamilli gave the impression that the private industry and nations should prioritize security into the future as the proliferation of digital culture dramatically changes the dynamics of the freedom vs. security debate.

Day-in-Summary Conversation:

The symposium concluded with a panel that included all of the day's participants. It was moderated by the symposium's keynote speaker, Liisa Past. The conversation allowed for the participants to provide closing remarks after participating on the panels and to communicate their major concerns with creating a sustainable world in tangent with the application of cybersecurity into the future.

Liisa Past asked the panel about what they considered to be the most pressing social, economic, and political issues that nations and the international community will need to solve in the future and how the digital realm and cybersecurity apply to these issues and possible outcomes.

Dr. Ford said that the biggest challenge, sustainability-wise, is the issue of the digital divide between developed and developing states. He also stated that governments and technology companies must work to resolve trust issues with the public to ensure the development of sustainable cybersecurity.

Megan Stifel also was concerned about the aspect of trust as it relates to the relationship between intermediaries (e.g. Facebook, Google), consumers, and governments. He said that disinformation efforts that are led by governments and individuals seek to sow fear, uncertainty, and doubt into consumers. Intermediaries and governments must work together to discover sustainable solutions.

Dr. Ray was mostly concerned about the issue of a loss of trust in cyberspace caused by nations and individuals. He fears that the spread of disinformation can lead to the rise of political figures

in nations that are more inclined to act upon authoritarian tendencies as trust in government institutions and with digital companies continues to evaporate.

Jackie Kerr was also interested in trust in cyberspace, but spent the time expanding upon the importance of civil society in a healthy democracy. She said that for democracies to form and sustain themselves in our new digital environment, online civil society must be safeguarded by sustaining legitimacy in the institutions that operate and regulate these spaces.

Dr. Von Welch was extremely concerned in the rapid proliferation of technological advances for average consumers. The rate of change in technology, as he stated, is currently not being met at the same pace with regulations to ensure that the public and governments are safeguarded against new and constantly-evolving cyber threats.

Dr. Shackleford concluded his remarks by drawing parallels between the concept of polycentric governance, which is governance that prioritizes the use of local resources, and the success of the Paris Climate Accords. He stated, as an optimist, that if governments follow this sustainable model, they standardize cybersecurity nationally, then regionally, and later, globally.

Marios Efthymiopoulos ended with both positives and negatives that will be driven by digital products into the future. In one view, big data and the interconnected world will bring people closer together than ever before and create new, lifesaving and life-enhancing technologies. He also recognized that laws need to be formulated to counter the negative aspects of technological change. He closed by advocating for intermediaries and governments to anticipate possible new laws before new technology is released.