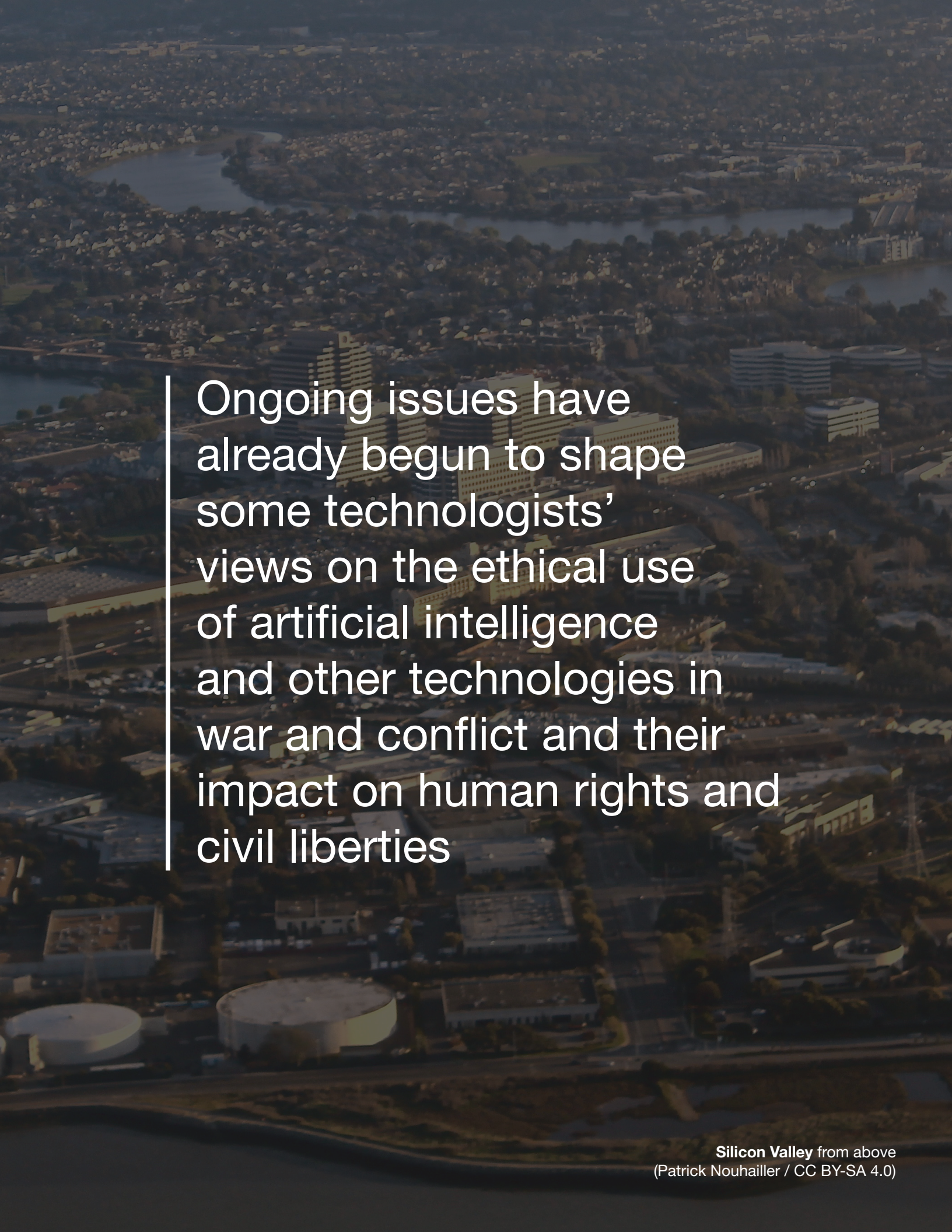


Ongoing issues have already begun to shape some technologists' views on the ethical use of artificial intelligence and other technologies in war and conflict and their impact on human rights and civil liberties

Silicon Valley from above
(Patrick Nouhailler / CC BY-SA 4.0)

A Healthier Way for the Security Community to Partner with Tech Companies

Dr. Douglas Yeung

Digital data captured from social media, cell phones, and other online activity has become an invaluable asset for security purposes. Online mapping or cell-phone location information can be used to collect intelligence on population movement, or to provide situational awareness in disasters or violent incidents. Social-media postings may be used to vet potential immigrants and job applicants, or to identify potential recruits who may be likely to join the military.

However, breakdowns in relationships between the tech industry and would-be consumers of technology's handiwork could imperil the ability of security stakeholders to use this data. Ongoing issues have already begun to shape some technologists' views on the ethical use of artificial intelligence and other technologies in war and conflict and their impact on human rights and civil liberties. It isn't difficult to imagine a series of future incidents further souring collaboration between technologists and security stakeholders.

In contrast to its reluctance over security matters, the tech industry has been a willing partner for government agencies and communities that promote health and wellbeing—topics that present less of an ethical challenge. Although it may not be immediately apparent, wellbeing and security have much in common. Could the security community take a page from wellbeing efforts to improve their collaboration with the tech industry?

BIG TECH HOLDS MOST OF THE CARDS

Maintaining data-sharing partnerships with the tech sector is critical to ensuring that security interests can access timely, representative, and complete data sets; build and operate robust data transfer pipelines; and maintain reliable data storage and backups. Properly interpreting data requires highly trained analysts and organizational support, analytic tools, and knowledge-sharing policies and protocols. Data must also be distributed to those who need it most—intelligence analysts, military commanders, and senior decision makers—and safeguarded against theft or loss. As with any security mission, interrupting the supply chain (in this case, digital data, its supporting infrastructure, and access to tools and trained personnel) can threaten the mission's success.

Given the market dominance of a few big companies, such as Amazon, Facebook, and Google, these digital assets and capabilities likely cannot be acquired through other channels. Social-media companies tightly control data access, while big data-management and analytic capabilities often reside in cloud-computing companies. As a result, tech companies have become critical security partners for governments and other stakeholders. As with allied nation-states or international coalitions, maintaining working relationships and cooperation is essential for continued data flows.

LACK OF TRUST IMPERILS TECH-SECURITY COLLABORATION

Perhaps the key challenge to these partnerships is a loss of trust resulting from a perceived mismatch in institutional goals between government security agencies and the tech companies on which these agencies have come to depend. Vocal tech workers have taken actions to block their employers from cooperating with government agencies or working on projects that the workers find objectionable. In 2013, leaks about the National Security Agency's (NSA) alleged data-collection activities strained relationships between the NSA and tech companies as well as members of Congress, foreign government leaders, and the public. After criticism from the public and their own employees, tech companies such as Yahoo, Google, Verizon, and Apple increased security measures, called for surveillance reform in a joint open letter expressing some distrust of the government, and released "transparency reports" that detailed the government's requests for information and how the companies responded (e.g., what type of information was shared).

More recently, Microsoft employees demanded that the company stop working with Immigration and Customs Enforcement to protest family separations at the U.S.-Mexico border.[1] Google employees signed a petition and some even resigned in protest over Google's work with the Department of Defense on artificial-intelligence capabilities for drones.[2] Amazon employees, citing family separations and government surveillance, objected to selling the company's facial-recognition software to law-enforcement agencies.[3] These companies have ended some security-related projects and may be wary of ongoing or future government cooperation on security matters.

Tech companies have taken other concrete actions such as hardening security protocols to impede law enforcement or intelligence agencies from intercepting communications, and either canceling or declining to bid on government defense contracts.

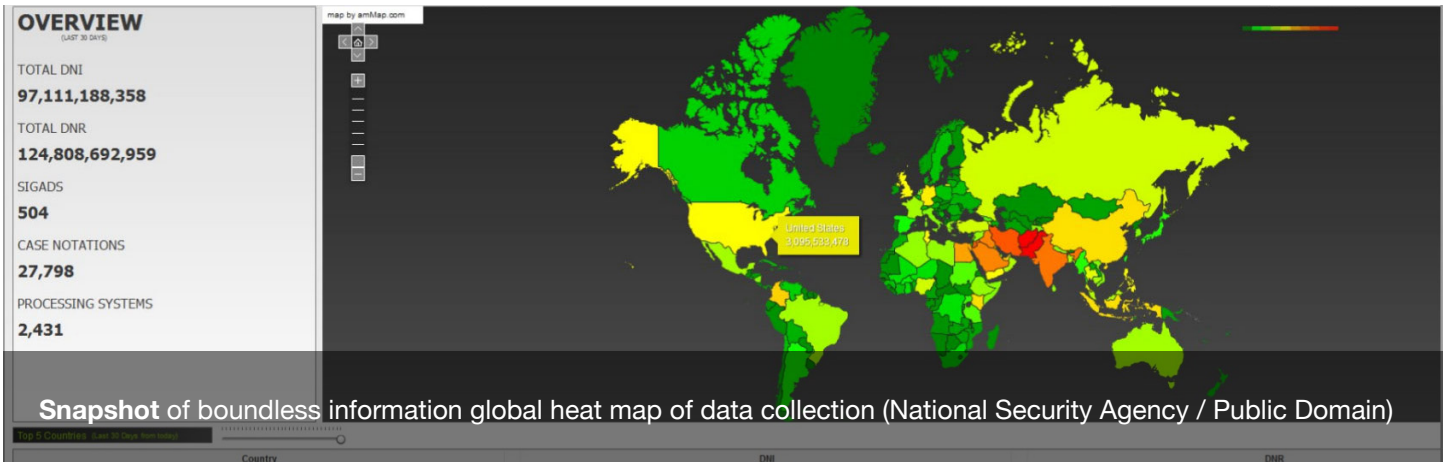
ADVANCING SECURITY THROUGH WELLBEING

There is another path to advancing security—one that piggybacks on the burgeoning public-private cooperation around civic wellbeing. Governments at all levels and in communities around the world are leading initiatives to improve collective wellbeing though the use of digital data. These efforts emphasize measuring how local conditions, policies, and programs influence quality of life, and promoting those that have the largest positive impact. The institutions at the forefront of these efforts have worked to ensure they are making the best use of technology-derived insights to address intractable societal problems.

These collaborations benefit from the tech industry's perceptions of their government partners. In contrast to security-related collaborations, the tech industry appears to hold a more positive view of the government's motivations when the goal is society's wellbeing.

Two examples illustrate how collaborations between local governments, tech companies, and other civic organizations have succeeded. Air Louisville, for instance, is a community partnership program that began in 2012 to provide local government with information about air quality in Jefferson County from sensors fitted to residents' asthma inhalers.[4] This data-driven collaboration between philanthropic funders, public agencies, and private tech companies mapped environmental conditions and corresponding health risks, and used that information to identify mitigating actions, such as rerouting trucks away from high-risk areas.

The City of Santa Monica's Wellbeing Project sought to go beyond traditional (e.g., economic) performance measures to measure government's impact on the wellbeing of its residents. Santa Monica's Wellbeing Index has engaged multiple partners to collect and make use of data and emerging technologies to provide a shared understanding of community strengths and needs. For example, the RAND Corporation, headquartered in Santa Monica, has worked to help Santa Monica measure civic wellbeing, partly through analyzing social-media data, and embed that information into policymaking. Santa Monica also partnered with RAND, Fitbit, and Fitabase, a research platform for health tools, to observe indicators related to physical activity or other factors of wellbeing. With more information about residents' health, Santa Monica plans to improve city planning and investments, and design programs and policies to improve resident wellbeing. In both cases, the city's



Snapshot of boundless information global heat map of data collection (National Security Agency / Public Domain)

tech partners likely joined the effort in part to advance wearables and other tech products that are positioned to play a role in digital health, telemedicine, and precision medicine.

WELLBEING AND SECURITY ARE COMPLEMENTARY DOMAINS

While the similarities may not be immediately apparent, wellbeing and security are, in fact, complementary concepts. Both involve societal institutions striving to ensure the safety and welfare of their citizens. Additionally, both include the notion of collective benefit, or that collective actions may not offer direct benefits to an individual or group but should be undertaken to advance the mutual interests of an entire community. Examples of this principle of shared responsibility for security include mutual defense treaties, security alliances and coalitions, and, for wellbeing, international bodies convened to tackle global health crises.

Similar to security efforts, wellbeing initiatives focus on understanding broad factors and upstream drivers that influence the state and stability of an entire community or group. Both domains attempt to build resilience to buffer the population against natural disasters, infrastructure catastrophes, terrorist attacks, or war. Programs and interventions in each domain create conditions that can fulfill more fundamental requirements for economic and physical security (e.g., physical infrastructure) as well as higher-order goals (e.g., public optimism). For instance, a foundational aspect of wellbeing is developing healthy attitudes and behaviors as well as a sense of community, each of which starts with creating shared values among community members.[5] Relatedly, counterinsurgency or other military campaigns may seek to "win hearts and minds," acknowledging the importance of gaining a population's trust.

Economic opportunity, which includes the availability of jobs, businesses, and affordable housing, is a critical component of both wellbeing and security because it provides people with financial security and stability. Concerns about financial security and a lack of prospects can hollow out a community, as young people move away to seek jobs, leaving less-mobile individuals behind and without support. Similarly, refugees and asylum seekers in search of a better life due to economic or safety concerns are often seen as a security threat or an economic burden. Yet research suggests that refugees and other migrants actually provide economic benefit to a region.[6] Wellbeing or security efforts that address economic vulnerability or humanitarian crises in potential migrants' home countries may slow their outflux, as improved community conditions allow people to thrive in place.

Similarly, wealth inequality presents a serious threat to both global stability and wellbeing. Prominent individuals such as former President Barack Obama, billionaire investor Warren Buffett, and Facebook CEO Mark Zuckerberg have all decried the detrimental economic impact of income inequality.[7] Some community wellbeing stakeholders have made addressing inequality an explicit goal, or even their central mission.[8] Increasingly, inequality is also seen as a multidimensional security challenge, such as by fueling populist sentiment.[9] Governments routinely undertake a wide range of security assistance, economic development, and other foreign aid programs, each with differing priorities and stated goals. Collectively, these programs could be viewed through the lens of addressing inequality.

Finally, population diversity benefits both wellbeing and security. It adds richness to societies, and it can improve creativity and performance in smaller groups. Military recruiting leaders, for example, emphasize the importance of creating a diverse mix within the armed forces that reflects the breadth of the general population.

HOW COULD A WELLBEING APPROACH BRIDGE THE TECH-MILITARY DIVIDE?

Given these commonalities, the question for security stakeholders is this: to what extent could they use digital data and other emerging technologies to better understand and monitor the health and security of communities, and then look to solve problems that are central to societal wellbeing? Digital data from tech-sector partnerships support several key functions for wellbeing that may also fulfill security requirements. For example, social-media content is useful to track public sentiment and to estimate political will. Geolocation data can provide information to allocate resources and position infrastructure. These and other forms of digital data are useful to provide situational awareness in preparation for disasters or unexpected events, and to inform forecasts and predict trends.

The U.S. government has begun to address this question

CSO of Headspace Dr. Megan Jones Bell (center) speaks at HealthConf (Web Summit / CC BY 4.0)

by increasing its outreach to and engagement with the tech community. Attempting to head off the potential loss of access to critical technologies, U.S. national security and intelligence agencies have established several Silicon Valley outposts (e.g., In-Q-Tel, Defense Innovation Unit) to increase their presence and build relationships in the tech community. Additionally, direct engagement on contentious topics could send a more powerful signal of openness. For instance, the mission of the Department of Defense's newly created Joint Artificial Intelligence Center emphasizes engaging artificial-intelligence researchers and developers on tech ethics and civil liberties.

Another potential avenue to bridging civil-military divides would be to explore how governments and tech partners have successfully collaborated on wellbeing in the past. How were tech and wellbeing collaborations forged, and what motivated tech companies' leaders and employees to join them? Tech companies may find it beneficial to signal that they are working productively to improve the wellbeing of a community, for example. As evidence, consider the existence of several wellbeing-focused corporate arms of tech companies, such as Google's Sidewalk Labs, Headspace Health, Uber Movement, and Airbnb Citizen. Tech companies, in contrast, may wish to signal to internal and external audiences that they are not cooperating on controversial uses of digital data. This may suggest that the security community should deliberately consider how potential collaborations or uses of digital data might be perceived by the public and the tech industry. It may also suggest that security stakeholders reframe or refocus their efforts on issues like inequality that cut across wellbeing and security. In this manner, tech and wellbeing could be a model for how to use tech productively to improve wellbeing and security, and for a less controversial path to tackling fraught or challenging issues.

CONCLUSION

Developing and harnessing technological innovation is an essential step on the path to advancing security. Whereas technological innovation was once limited to the nation-state, today it often resides in private companies across the world. Debates have erupted over the appropriate use of this technology, and these disagreements threaten the continued ability of governments and other security stakeholders to develop advanced capabilities. On the other hand, attracted by the potential for digital data to inform policymaking and improve decision making, a growing number of governments and nongovernmental institutions have successfully partnered with the private sector to analyze this data as a means of increasing societal wellbeing.

Existing efforts to promote community health and wellbeing have included stakeholders from sectors as varied as transportation and business. These initiatives have also begun reaching out to the defense and security communities, which have a longstanding interest in the health and resilience of military families and communities. Not only is wellbeing neatly complementary to security efforts, but also many security actors have long recognized the importance of wellbeing and have been engaging in wellbeing promotion for years. The U.S. military has sought to support the economic opportunities available to military caregivers, address servicemember mental health, assess "comprehensive soldier fitness," and examine the impact of communication technologies on service members' resilience and wellbeing.[10] The parties involved in these combined efforts could consider how to expand this outreach and strengthen these relationships.

Any efforts to capture and derive value from digital data, whether it is wellbeing- or security-focused, will likely have to grapple with a set of common concerns. As is clear from recent trends, tech ethics and data privacy, along with equity and bias in algorithms, will probably remain among such concerns. Further, while security stakeholders must contend with the private sector's wariness, digital data companies are facing their own reckoning in terms of public trust. Addressing these issues will be important in determining the feasibility and success of future collaborations on tech and security.

Seen from another angle, the major security challenges facing the world may end up resembling wellbeing problems. Automation and a resulting lack of work and opportunity may threaten people's sense of meaning and purpose. Unaddressed mental health issues may precipitate violent incidents. Mass migration can spark regional conflicts. Online hacking and trolling contribute to a breakdown of civic trust and participation and weaken our belief in facts and evidence. Climate change could more frequently spawn severe, deadly weather events.

Ensuring security is the most fundamental responsibility of government. The ability to discharge that responsibility will benefit from continued collaborations with the tech industry and other societal actors to acquire and employ technological capabilities. Security stakeholders already cooperate with a wide range of actors across different countries and with different missions. Going forward, the security and wellbeing communities should consider how the similarities of their missions can inform the best use of digital data to achieve security and wellbeing for all.

[1] Sheera Frenkel, "Microsoft Employees Protest Work With ICE, as Tech Industry Mobilizes Over Immigration," The New York Times, June 19, 2018, <https://www.nytimes.com/2018/06/19/technology/tech-companies-immigration-border.html> (accessed January 17, 2019).
[2] Daisuke Wakabayashi and Scott Shane, "Google Will Not Renew Pentagon Contract That Upset Employees," The New York Times, June 1, 2018, <https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html> (accessed January 17, 2019).
[3] See: James Vincent, "Amazon employees protest sale of facial recognition software to police," The Verge, June 22, 2018, <https://www.theverge.com/2018/6/22/17492106/amazon-ice-facial-recognition-internal-letter-protest> (accessed January 17, 2019); Ali Breland, "Amazon employees protest sale of facial recognition tech to law enforcement," The Hill, June 21, 2018, <https://thehill.com/business-a-lobbying/393583-amazon-employees-protest-sale-of-facial-recognition-tech-to-law> (accessed January 17, 2019).
[4] "Homepage," Air Louisville, <https://www.airlouisville.com> (accessed January 17, 2019).
[5] "Making Health a Shared Value," Robert Wood Johnson Foundation, <https://www.rwjf.org/en/cultureofhealth/taking-action/making-health-a-shared-value.html> (accessed January 17, 2019).
[6] See: Amy Maxmen, "Migrants and refugees are good for economies," Nature, June 20, 2018, <https://www.nature.com/articles/d41586-018-05507-0> (accessed January 17, 2019); J. Edward Taylor, Mateusz J. Filipski, Mohamad Alloush, Anubhab Gupta, Ruben Irvin Rojas Valdes, and Ernesto Gonzalez-Estrada, "Economic impact of refugees," Proceedings of the National Academy of Sciences of the United States of America 113 (27) (July 5, 2017): 7449–7453.
[7] Catherine Clifford, "Obama on wealth inequality: 'There's only so much you can eat. There's only so big a house you can have.,'" CNBC, July 18, 2018, <https://www.cnbc.com/2018/07/18/barack-obama-on-wealth-inequality-only-so-much-you-can-eat.html> (accessed January 17, 2019).
[8] "Outcome: Improved Population Health, Well-being, and Equity," Robert Wood Johnson Foundation, <https://www.rwjf.org/en/cultureofhealth/taking-action/outcome-improved-population-health--well-being--and-equity.html> (accessed January 17, 2019); Darren Walker, "Toward a new gospel of wealth," Ford Foundation, October 1, 2015, <https://www.fordfoundation.org/ideas/equals-change-blog/posts/toward-a-new-gospel-of-wealth> (accessed January 17, 2019).
[9] Brenda M. Seaver, "This Is Why Global Income Inequality Is a Real National-Security Threat," The National Interest, September 1, 2015, <https://nationalinterest.org/feature/why-global-income-inequality-real-national-security-threat-13747> (accessed January 17, 2019).
[10] "Comprehensive Soldier & Family Fitness," U.S. Army, <http://csf2.army.mil> (accessed January 17, 2019); Laura L. Miller, Laurie T. Martin, Douglas Yeung, Matthew Trujillo, and Martha J. Timmer, Information and Communication Technologies to Promote Social and Psychological Well-Being in the Air Force: A 2012 Survey of Airmen (Santa Monica: RAND Corporation, 2014), 104.

Dr. Douglas Yeung

Dr. Douglas Yeung is a behavioral scientist at the RAND Corporation and a member of the Pardee RAND Graduate School faculty. His research examines the societal impact of technology in national security, workforce, and wellbeing policy. His recent work has explored how policymakers can use insight from emerging technologies (e.g., social media, mobile devices) for wellbeing and civic policy-making. Yeung's other research involves online professional communities, and explores workforce attitudes and organizational knowledge-sharing, such as how military recruits discuss and seek career information. He has also conducted workforce diversity research, such as how minorities and women perceive career options. He has published most recently on public trust in the tech industry, and intentional bias in algorithms.

Before coming to RAND, Yeung was a product analyst at Oracle, and also helped to create a mobile application that was a grand prize winner in Google's first Android Developer Challenge. He received a Ph.D. from Rutgers University - Newark, and a B.S. from the Massachusetts Institute of Technology.