Toward a Human-Centric Approach to Cybersecurity

*Ronald J. Deibert**

Experts often note that while there is widespread consensus around the importance of cybersecurity, there is very little agreement on how to approach it. Indeed, even the very definition of "cybersecurity" is deeply contested. A database maintained by the Washington, D.C., think-tank New America lists more than 400 unique definitions.[1] While there is a healthy plurality of proposed views, actual practices are coalescing around a dominant "national security–centric" approach to cybersecurity.[2] Such an approach places the sovereign state as the principal object of security. Derived from a realist theory of world politics in which states compete with each other for survival and relative advantage, the principal cybersecurity threats are conceived as those affecting sovereign states, such as damage to critical infrastructure within their territorial jurisdictions. This approach delegates responsibility for the security of cyberspace to military, intelligence, and law enforcement agencies, which together constitute the state's national security apparatus. These agencies tend to operate with limited public accountability, oversight, and transparency.

Though it dominates the conversation even in Western democracies, the "national security first" approach to cybersecurity is most compatible with authoritarian and illiberal practices, which are on the rise worldwide.[3] Numerous governments have used the exigencies of cybersecurity to justify vast Internet censorship regimes, extensive surveillance programs, international cyber espionage, disinformation campaigns targeting regime critics, and draconian legislation that limits freedom of expression online, labels dissent as "fake news," and compels companies to locate data in their jurisdictions for efficient state access.[4]

*I am grateful to Tim Maurer, Duncan Hollis, the editors of *Ethics & International Affairs*, Christopher Parsons, Cynthia Kloo, Lex Gill, Irene Poetranto, and Adam Molnar for helpful comments, and to Liz Gross for research assistance.

Ethics & International Affairs, 32, no. 4 (2018), pp. 411–424.

doi:10.1017/S0892679418000618

There is, however, an alternative: the human-centric approach. A human-centric approach draws inspiration from principles of liberalism and republican thought going back to the Enlightenment, the early Middle Ages, and even ancient Greece.[5] It places human beings, regardless of nationality or citizenship, as the primary objects of security.[6] Rather than prioritizing the territorial sovereignty of networks, this approach views networks as part of the essential foundation for the modern exercise of human rights, such as access to information, freedom of thought, and freedom of association. Sovereign states still have an important role to play, but as supporting institutions whose purpose is the protection of individuals' rights and wellbeing. Though in the minority, some policymakers, businesses, and civil society organizations have advocated for this type of approach. The Freedom Online Coalition, for example—a group of thirty national governments[7]—has formally endorsed a collective commitment to Internet openness and respect for human rights online.[8]

In what follows, I elaborate on some of the foundational elements of a human-centric approach to cybersecurity and contrast those elements with the prevailing trends around national security–centric practices.[9] First, I outline the way in which a human-centric approach conceives of the role of international law and state sovereignty as it relates to cybersecurity, and specifically how this approach prioritizes human rights and civil society as the ultimate objects of security, with nation-states in supporting roles. I then examine four important issue areas—network security, Internet censorship, data stewardship and privacy, and human rights enforcement—and show how governance in these areas would have to change under a human-centric approach. A human-centric approach to cybersecurity fundamentally rests on a political architecture of "distributed security," at the heart of which are institutional mechanisms of power restraint most often associated with the concept of "checks and balances." While it may be discouraging to see how far removed existing practices are from human-centered ideals, elaborating on these principles provides a road map of goals and a yardstick by which to hold actors to account.

International Law and Cybersecurity: Prioritizing Human Rights

At the core of a human-centric approach to cybersecurity is the principle that all cybersecurity laws, policies, and practices should respect international human

https://doi.org/10.1017/S0892679418000618 Published online by Cambridge University Press

rights and humanitarian laws. Since its inception, there has been an ongoing debate as to whether cyberspace constitutes a unique domain such that an entirely new body of law is needed to regulate it or whether existing laws can and should be applied.[10] However, several international forums and expert legal groups, including the United Nations Human Rights Council (2012), the UN Group of Governmental Experts (2013), the Freedom Online Coalition (2016), and various UN Special Rapporteurs have all affirmed that current international law should apply online (in cyberspace) just as it does off-line. Likewise, it is now widely recognized that international humanitarian law should apply to what has been called "armed conflict" in and through cyberspace, including "limitations on the use of indiscriminate weapons, distinction between military targets and civilians, proportionality, and perfidy."[11] A human-centric perspective conforms with these positions.

International law pertains, first and foremost, to the principled conduct of sovereign states in their relations with each other. But who should be the ultimate beneficiary of international law: sovereign states themselves or the individuals that make up those sovereign states? A human-centric approach to cybersecurity falls squarely on the side of the latter perspective, that the "international rule of law ought to benefit individuals in priority and sovereign states are agents of that entitlement."[12] From a human-centric view, it is "appropriate to think of national sovereigns more as 'officials' or 'agencies' of the [international legal] system than as its subjects."[13] The distinction is important to cybersecurity for several reasons. First, there is (as with much else in world politics) a divergence between principles and practices when it comes to state behavior in cyberspace. While China, Russia, the United States, and many other countries have formally endorsed legal principles about appropriate conduct in cyberspace, all of them routinely violate them in practice.

Second, the distinction illustrates a central tension between national security–centric and human-centric approaches. Viewing sovereign states as the primary object of international law fits comfortably into and reinforces a national security–centric approach to cybersecurity in which military, intelligence, and other security agencies take the lead and in which the state is the ultimate source of authority. In spite of disputes between them, national security agencies of even adversarial states share common traits: they are typically subject to limited oversight and accountability, and are historically separated from the citizenry by secrecy, hierarchy, and virtually unchecked executive power. With these agencies

taking the lead on cybersecurity, sovereign state interests can be reified as ends unto themselves. Meanwhile, other principles and values, such as human rights, take a back seat and are typically relegated to marginal discussions.

Third, the distinction matters because the tension described above carries over into the domestic sphere, as international law imposes obligations on states that, in turn, affect their domestic constitution and behavior. Under the prevailing national-security paradigm, states prioritize pursuing and indicting perpetrators of cybercrimes that have an impact on state security. Under the human-centric approach, governments would be obligated to protect and extend human rights, including enacting and enforcing human rights–related laws, and requiring businesses headquartered in their jurisdictions to respect human rights as they operate abroad. Indictments could be expected against foreign hackers for cyber espionage against journalists, activists, and human rights defenders as often as they are now made against foreign hackers for cyber espionage against governments or the private sector.

Finally, the question of whether states or individuals are the primary beneficiaries of international law informs how we analogize domestic and international governance. The protection of human rights requires by necessity the separation of political power through formal mechanisms of mutual restraint (checks and balances) that extend from the domestic sphere out into the international realm, giving substantive depth to the otherwise shallow notion of "multistakeholderism."[14] Far too often in international governance the inclusion of civil society is treated like an act of charity, their inputs mere reminders of some distant moral purpose separate from the serious business of real-world, hard-power politics. From a human-centric point of view, ensuring a cross section of participants in international governance arrangements is more than a superficial hat tip to pluralism; it is an essential, constitutive ingredient in the restraint of political power.

Network Security

With data surrounding us and networked into everything we do, the security of our data, both in transit and while at rest, is an obvious public safety issue, which makes it puzzling why governments—whose principal job is to keep their citizens safe—have repeatedly sought to deliberately weaken the protocols that secure citizens' data. As with much else, the root of this seeming paradox can ultimately be traced to differences in threat paradigms: differences between what (or

https://doi.org/10.1017/S0892679418000618 Published online by Cambridge University Press

who) are considered the principal objects of security (meaning, that which is to be protected).[15] Is it the state, or is it the people? Is it the network within a particular sovereign territorial space, or is it the undifferentiated global network as a whole?

A human-centric approach to cybersecurity squarely falls in the latter camp, and would strive to ensure that all laws, policies, and practices uphold the integrity of communication systems worldwide—from code to physical infrastructure and everything between (all of which are referred to here, in abbreviated form, as "networks"). A by-product of this approach would be preventing government policies that would deliberately impede technological developments that protect data and users' security, including encryption. The logic of this approach rests on an appreciation of the constitutive role that communication technologies play in all human activity, and in particular how communication technologies can shape and constrain the possibilities for human choice and action. Policies that deliberately introduce weaknesses or other distortions into these networks can adversely affect the exercise of human rights.

To be sure, there may still be times when public safety agencies will require exceptions to these rules, and such exceptions should be handled with as much transparency as possible. One model for this is the "vulnerabilities equities process" used by the U.S. government: a case-by-case approach to whether it should disclose or harbor knowledge of software vulnerabilities in the interest of public safety.[16] However the process is organized, at a minimum a human-centric approach would require exceptions to be limited, proportional, and transparently justified to the public. From a human-centric approach, the network as a whole must be secured for all users, regardless of territorial boundaries.

Historically, power competition among states has involved governments using various forms of cryptography to protect their communications while simultaneously striving to crack each other's secret codes. While these state-versus-state contests may have made sense when the world was neatly divided into territorially segmented communication spaces, they no longer do. Increasingly, governments, companies, and citizens all over the world rely on the same communication technologies and networks. Thus, when government agencies deliberately weaken cryptographic protocols in such a system to gain momentary advantage over their opponents, they do so at the expense of their own citizens' security.

National security concerns are not the only motivation for government agencies to weaken network security. Like intelligence agencies, law enforcement has also sought to keep cryptography controlled or deliberately compromised, but for

them the principal concern is being able to investigate criminal behavior, whether through mass surveillance or surreptitious access to a criminal's smartphone.[17] Here again, however, we see a similar problem as above. Criminals and law-abiding citizens alike use the same communication systems: weaken them for one and you weaken them for all. There is also a risk that criminals will adopt foreign-developed strong encryption while law-abiding citizens will continue using the weakened cryptographic systems that can be exploited by law enforcement, criminal groups, and foreign national security agencies alike.

Time and again, government officials have used national security or lawful access justifications to argue for restrictions or special "back doors" on encryption.[18] Time and again, computer scientists, engineers, and rights activists have argued the opposite.[19] In a world in which networked devices and sensors are increasingly inseparable from any and all human activity, the proper exercise of human rights requires that those systems be as secure as possible. A human-centric approach to cybersecurity would thus insulate technological research, design, and development as much as possible from narrow national security interests and other machinations, and devote legal, financial, and other resources to raising the bar for everyone's cybersecurity—regardless of location or jurisdiction.

Internet Censorship

Access to information and freedom of association are central pillars of human rights. A human-centric approach to securing cyberspace would prioritize unrestricted access to networks as a fundamental component of cybersecurity. At the core of this approach would be the principle that no matter where or how a person accesses the Internet, once connected, that person should enjoy access to the same information as any other person.

While the publicly accessible Internet was originally designed to facilitate seamless information sharing, as it has grown so too have concerns over access to controversial content, leading to various types of restrictions. Internet censorship is now routinely practiced—in schools, libraries, businesses, and on a national scale. A growing number of countries now require companies to filter, throttle (slow down), or otherwise interfere with access to the Internet, including liberal democratic countries.[20] Controlling information is also big business: cybersecurity companies, such as Canada's Netsweeper or the U.S.-based Blue Coat Systems, make millions selling technologies that restrict access to information on behalf of governments.

https://doi.org/10.1017/S0892679418000618 Published online by Cambridge University Press

Internet censorship can take place at different points across the network, and with varying degrees of transparency. In China, for example, Internet companies are required to censor their users, monitor chats and forums, and share information with security services on demand. This not only means that information controls extend into the application layer of the Internet but also that Internet users experience a diversity of information controls depending on how they connect.

Internet censorship can also be targeted in response to specific events, such as controversial anniversaries, elections, demonstrations, or discussion of sensitive topics. The most drastic form of information control is when the Internet is shut down entirely for a limited period in response to a specific event—what my OpenNet Initiative colleagues and I have defined as "just-in-time" blocking.[21] The practice allows governments to heavily restrict information flows during strategically important time periods for their political opponents. Access Now, an Internet advocacy group that has been tracking Internet shutdowns as part of its "#KeepitOn" campaign,[22] found at least 75 instances of Internet shutdowns in 2016, and 108 instances in the first three quarters of 2017. Shutdowns can be targeted to occur in specific regions or even neighborhoods, and can affect specific services or applications.

A human-centric approach to cybersecurity would eliminate these types of network interferences, with some important exceptions. The protection of human security will require balancing competing rights, such as the right to communicate freely versus the right to be free from fear or hatred. In a human-centric approach to cybersecurity, there will be circumstances in which access to content should be legitimately restricted, or even removed from the network altogether, because of sensitivities to these other rights. Restrictions on the circulation of child pornography or content that incites genocide are two obvious examples that most adherents to a human-centric approach would agree require controls. However, a human-centric approach would ensure that such measures are exceptions to the rule, undertaken according to laws that limit collateral damage, notify affected parties, and provide suitable avenues for recourse.

Data Stewardship and Privacy

We are in the midst of one of the most profound shifts in human social and economic relations as a consequence of the growing use of digital technologies, especially social media. Within a span of a few short years we have collectively

turned our lives inside out as a new model of political economy—the personal data surveillance economy—has taken hold. At its core, this model involves the provision of free services in exchange for the collection of highly detailed, fine-grained data from a vast number of individuals for the purposes of acquiring advertising income. We now emit a constant stream of data from our always-connected devices that surround us in our workplaces, homes, modes of transportation, and even in our pockets. These data streams are harvested, analyzed, and repurposed to make predictions about us and ultimately to shape our behavior. As this data is integrated and analyzed using increasingly sophisticated algorithms and computational power, an overall system emerges that can limit our freedom of choice, thought, and association.[23] When companies share this data with governments, the system can become an existential threat to users. As an extreme example, in China the government and private sector are now working together to create a "social credit" system that will rank citizens' reliability according to their off-line and online behavior. Those who behave in ways contrary to regime interests might discover their ability to get a loan, find work, or travel abroad to be constrained.[24]

Securing human rights amid this tectonic shift must be essential to a human-centric approach to cybersecurity. Traditionally, such concerns would be discussed under the rubric of a right to privacy, a concept that has its origins in modern Europe, pertaining principally to societies that were then more neatly compartmentalized into "inside" and "outside," or "public" and "private" categories. As these distinctions lose their significance in practice, a more expansive notion of *data stewardship* is required as part of a human-centric approach to cybersecurity. Data stewardship involves citizens' control over their personal data, enforced by real authority and legal consequences. Although it is common to contrast "privacy" with "security"—especially by state agencies following the national security–centric view of cybersecurity—a human-centric approach would abolish this distinction, effectively converting "privacy" into one component of its own form of security. In today's highly networked societies, in which an individual's personal data is widely distributed across numerous platforms, securing privacy requires a comprehensive approach in which individuals are empowered to control what happens to their data no matter where it is located, and governments and companies should have legal obligations to treat data in ways that protect the privacy of all users and citizens—thus promoting *human* security.

At present, the best examples of enforcement mechanisms are government-created independent oversight agencies and privacy or data protection commissioners, such as the U.S. Federal Trade Commission and the Privacy Commissioner of Canada. However, some of these agencies tend to be understaffed and to lack meaningful authority and power to investigate, compel cooperation, and punish those who commit offenses—especially outside their national jurisdictions. Meanwhile, billions of dollars flow to largely unaccountable national security agencies as part of cybersecurity programming. A human-centric approach would devote at least as much, if not more, resources to independent agencies at multiple levels of governance with real teeth working on behalf of citizen and user data security. It would involve having strong privacy commissioners who would be authorized to investigate data stewardship practices and to levy fines or other penalties for violations of human rights, including for companies headquartered outside their jurisdictions. It would also include legal obligations on companies to disclose data breaches, to be liable for misuse of user data, and to be compelled to disclose any sharing of user data with third parties, particularly governments. The European General Data Protection Regulation is one promising example of such an approach.

Beyond legal obligations, a human-centric approach to cybersecurity would also encourage greater corporate social responsibility on the part of the private sector, following principles such as those outlined in the UN Guiding Principles on Business and Human Rights. Among those principles, states have a duty to "protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises" (Principle 1); and "should set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operations" (Principle 2), including extraterritorially. However, businesses also have a responsibility independent of governments to respect human rights. This corporate responsibility "exists over and above compliance with national laws and regulations protecting human rights" (Principle 11). Private companies have responsibilities to "avoid causing or contributing to adverse human rights impacts," and to prevent or mitigate adverse impacts "directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts" (Principle 13).

Generally speaking, the information and technology sector has only paid lip service to such principles, particularly regarding cybersecurity. In the absence of

restrictions against selling such technologies to governments with poor human rights records, there have been numerous documented cases of the abuse of spyware and other surveillance technologies. Microsoft's proposal for a "Digital Geneva Convention," although criticized by some for being self-serving and confusing, is nonetheless a promising example of the type of corporate social responsibility that a human-centric approach to cybersecurity would encourage.[25] Measures taken by companies such as Google to warn users of state-sponsored attacks or to provide easy-to-use digital hygiene tools are another. While necessary, such corporate social responsibility measures are unlikely to be sufficient, and the meaningful legal obligations outlined above will still be required. The bottom line is that as the public sphere becomes increasingly privatized, the private sector must be motivated by more than mere commercial concerns.[26]

Human Rights Enforcement Online

Of course, governments and companies routinely violate human rights online, and will do so into the future regardless of the progress made around human-centric values. That makes it all the more critical that our political and technical infrastructure is designed to promote, rather than neglect or override, human rights and similar human-centric values. A robust human-centric approach would include multiple, distributed organizations that undertake rigorous, evidence-based, and independent investigations into human rights violations in cyberspace and seek to protect the health and integrity of networks regardless of borders—a kind of cyberspace arms control, broadly understood. In the early days of the Internet, computer emergency response teams (CERTs) fulfilled this function. The first CERTs were established in the late 1980s and early 1990s, after a devastating Internet worm crippled systems worldwide. Most of the early CERTs were housed at universities and research centers, carrying with them academic norms of peer review, mutual support, information sharing, and trusted relationships on the basis of evidence and reputation. Over time, however, as the national security–centric paradigm has prevailed, many CERTs have lost their autonomy, having been drawn into the orbit of the national security apparatus; and in turn, this has affected their independence and relationships of mutual trust.[27] A human-centric approach to cybersecurity would aim to recover this independence, chartering such watchdog agencies in a way that their principal purpose is the health of networks regardless of national interests and other political interferences.[28] Such

https://doi.org/10.1017/S0892679418000618 Published online by Cambridge University Press

an approach would also necessitate the elimination of the now paradoxical situation in which cyber defense and offense missions are housed in the same agencies, as in Canada, the United Kingdom, the United States, and other countries.[29]

Universities may be one important home for such a distributed and independent watchdog function.[30] It was within the university system that the Internet was born and from which its guiding principles of peer review and transparency were founded. Protected by academic freedom, equipped with advanced research resources that span the social and natural sciences, and distributed across the planet, university-based research networks could be the ultimate custodians and independent monitors of an open and secure commons. Rigorous, evidence-based research is a powerful means by which to shed light on what is happening beneath the surface, whether the latter involves proprietary algorithms, commercial spyware, or state surveillance. An essential part of a human-centric approach would therefore involve persistent critical interrogation, including reverse engineering, of both technologies and the institutions that promote and sustain them. This should not only be seen as a right of inquiry but also as an essential ingredient of a critical democratic society. Research that "lifts the lid off" the technology that surrounds us to reveal hidden security and privacy risks is essential to human rights, regardless of whether companies bristle at the exposure or threaten legal action.[31]

Conclusion

We are at a crossroads in cyberspace. Mounting threats, an escalating arms race, and compounding data insecurity are compelling politicians to take action. In the face of such threats, the national security–centric approach to cybersecurity is holding sway, funneling resources, power, and authority to the least democratically accountable agencies. The ominous combination of the personal data surveillance economy and national security–centric approaches to cybersecurity threaten to stifle liberal democracy.

There is, therefore, an urgent need for a compelling counter-narrative to the reflex of nation-state control. A human-centric approach to cybersecurity supplies such a narrative, conceiving of our communications ecosystem as an essential arena for the exercise of human rights, including access to information and freedom of thought and association. As a consequence, it strives for indivisible network security on a planetary scale for the widest possible scope of human

experience, and would ensure that such principles are vigorously monitored and defended by multiple and overlapping forms of independent oversight and review.

To be sure, there are steep hurdles in the way of progress toward such a paradigm. Simply articulating the principles of human security will not immediately cease the raw exercise of power and competitive advantage in cyberspace. However, it will help raise the bar, set standards for progress, and challenge stakeholders to justify their actions in more than self-interested terms. Above all else, it will help focus collective attention on how best to sustain a common communications environment in which rights are protected in an increasingly compressed political space.

NOTES

[1] "Global Cyber Definitions Database," New America, Cyber Security Initiative (2014), cyberdefinitions.newamerica.org/.

[2] Yet another approach to cybersecurity that contrasts with both national security and human-centric approaches is one that is focused around corporate security and the maximization of profits, with a company's intellectual property and the unfettered flow of financial information being the object of security. I outlined this paradigm of cybersecurity in a 2002 chapter entitled "Circuits of Power: Security in the Internet Environment," in James Rosenau and J. P. Singh, eds., *Information Technologies and Global Politics: The Changing Scope of Power and Governance* (Albany, N.Y.: SUNY Press, 2002), pp. 115–42." For brevity, I focus here mostly on the contrast between national security and human-centric approaches.

[3] Marlies Glasius, "What Authoritarianism Is…and Is Not: A Practice Perspective," *International Affairs* 94, no. 3 (2018), pp. 515–33.

[4] Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds., *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, Mass.: MIT Press, 2010); and Ronald J. Deibert, "Authoritarianism Goes Global: Cyberspace Under Siege," *Journal of Democracy* 26, no. 3 (2015), pp. 64–78.

[5] Daniel Deudney, *Bounding Power: Republican Security Theory from the Polis to the Global Village* (Princeton, N.J.: Princeton University Press, 2007).

[6] For an overview of the concept of human security, see Roland Paris, "Human Security: Paradigm Shift or Hot Air?" *International Security* 26, no. 2 (2001), pp. 87–102.

[7] "About Us," Freedom Online Coalition website, freedomonlinecoalition.com/about-us/.

[8] Freedom Online Coalition Working Group 1, "An Internet Free and Secure," *Recommendations for Human Rights Based Approaches to Cybersecurity*, Freedom Online Coalition, September 21, 2015, www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Recommendations-Final-21Sept-2015.pdf.

[9] For a complementary view, see Myriam Dunn Cavelty, "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities," *Science and Engineering Ethics* 20, no. 3 (2014), pp. 701–715.

[10] Joel Reidenberg, "Governing Networks and Cyberspace Rule-Making," *Emory Law Journal* 45, no. 3 (1996), p. 911.

[11] International Committee of the Red Cross, "Cyber Warfare," October 29, 2010, www.icrc.org/en/document/cyber-warfare.

[12] Samantha Besson, "Sovereignty, International Law and Democracy," *European Journal of International Law* 22, no. 2 (2011), p. 373–87.

[13] Jeremy Waldron, "Are Sovereigns Entitled to the Benefit of the International Rule of Law?" NYU School of Law, Public Law Research Paper No. 09-01 (2009), papers.ssrn.com/sol3/papers.cfm?abstract_id=1323383##.

[14] Deudney, *Bounding Power*.

[15] Ronald J. Deibert, "Trajectories for Future Cybersecurity Research," in Alexandra Gheciu and William C. Wohlforth, eds., *The Oxford Handbook of International Security* (New York: Oxford University Press, 2018).

[16] United States White House, "Vulnerabilities Equities Policy and Process for the United States Government," November 15, 2017 (accessed August 10, 2018), www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[17] Dustin Volz, "FBI Chief Calls Unbreakable Encryption 'Urgent Public Safety Issue,'" *Reuters*, January 9, 2018, www.reuters.com/article/us-usa-cyber-fbi/fbi-chief-calls-unbreakable-encryption-urgent-public-safety-issue-idUSKBN1EY1S7.

[18] Chris Duckett, "Encryption Leaves Authorities 'Not in a Good Place': Former US Intelligence Chief," *ZDNet*, June 7, 2017, www.zdnet.com/article/encryption-leaves-authorities-not-in-a-good-place-former-us-intelligence-chief/; and Don Reisinger, "James Comey on Apple and Google's Data Encryption: They 'Drove Me Crazy,'" *Fortune*, April 16, 2018, fortune.com/2018/04/16/james-comey-apple-google-data-encryption/.

[19] Fred Cate and Jon Eisenberg, "NAS Report: A New Light in the Debate over Government Access to Encrypted Content," *Lawfare* (blog), February 15, 2018, www.lawfareblog.com/nas-report-new-light-debate-over-government-access-encrypted-content; and David Ruiz, "There Is No Middle Ground on Encryption," Electronic Frontier Foundation, May 2, 2018, www.eff.org/deeplinks/2018/05/there-no-middle-ground-encryption.

[20] Internet Society, "Internet Society Perspectives on Internet Content Blocking: An Overview," March 24, 2017, www.internetsociety.org/resources/doc/2017/internet-content-blocking/.

[21] Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds., *Access Denied: The Practice and Policy of Global Internet Filtering* (Cambridge, Mass.: MIT Press, 2008).

[22] "#KeepItOn," Access Now website (accessed July 12, 2018), www.accessnow.org/keepiton/#problem.

[23] Eileen Donahoe, "So Software Has Eaten the World: What Does It Mean for Human Rights, Security & Governance?" *Just Security*, March 18, 2016, www.justsecurity.org/30046/software-eaten-world-human-rights-security-governance/.

[24] Lotus Ruan, "When the Winner Takes it All: Big Data in China and the Battle for Privacy," Australian Strategic Policy Institute, Issues Paper, Report No. 5/2018, www.aspi.org.au/report/big-data-china-and-battle-privacy.

[25] Maria Gurova, "The Proposed 'Digital Geneva' Convention: Towards an Inclusive Public-Private Agreement on Cyberspace?" Geneva Centre for Security Policy, July 2017, www.gcsp.ch/News-Knowledge/Publications/The-Proposed-Digital-Geneva-Convention-Towards-an-Inclusive-Public-Private-Agreement-on-Cyberspace.

[26] For an elaboration of these themes with respect to private contracting of cybersecurity, see Kristen Eichensehr, "Public-Private Cybersecurity," *Texas Law Review* 95, no. 3 (2017), pp. 467–538; UCLA School of Law, Public Law Research Paper No. 16-47, ssrn.com/abstract=2847173.

[27] Robert Morgus, Isabel Skierka, Mirko Hohmann, and Tim Maurer, "National CSIRTs and Their Role in Computer Security Incident Response," Working Paper 2, New America, November 2015, www.digital-debates.org/fileadmin/media/cyber/National_CSIRTs_and_Their_Role_in_Computer_Security_Incident_Response__November_2015_--_Morgus__Skierka__Hohmann__Maurer.pdf.

[28] For more, see Samantha Bradshaw, "Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity," Global Commission on Internet Governance, Paper Series: No. 23, December 2015, www.cigionline.org/sites/default/files/gcig_no23web_0.pdf.

[29] Ronald J. Deibert, "The Cyber Security Syndrome," *OpenCanada.org*, November 25, 2014, opencanada.org/features/the-cyber-security-syndrome/.

[30] Ronald J. Deibert, "Towards Stewardship in Cyberspace," Citizen Lab and Canada Centre for Global Security Studies, Munk School of Global Affairs, University of Toronto, March 2012, www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_Deibert.pdf.

[31] That the university will remain a free space for such inquiries is hardly guaranteed, as both commercial and national security interests continuously present threats to academic freedom, and these are, arguably, growing.

Abstract: A "national security–centric" approach currently dominates cybersecurity policies and practices. Derived from a realist theory of world politics in which states compete with each other for survival and relative advantage, the principal cybersecurity threats are conceived as those affecting sovereign states, such as damage to critical infrastructure within their territorial jurisdictions. As part of a roundtable on "Competing Visions for Cyberspace," this essay presents

an alternative approach to cybersecurity that is derived from the tradition of "human security." Rather than prioritizing territorial sovereignty, this approach prioritizes the individual, and views networks as part of the essential foundation for the modern exercise of human rights, such as access to information, freedom of thought, and freedom of association. The foundational elements of a human-centric approach to cybersecurity are outlined and contrasted with the prevailing trends around national security–centric practices. A human-centric approach strives for indivisible network security on a planetary scale for the widest possible scope of human experience, and seeks to ensure that such principles are vigorously monitored and defended by multiple and overlapping forms of independent oversight and review.

Keywords: cybersecurity, human rights, human security, civil society, privacy, Internet governance