Cybersecurity Convergence: Digital Human and National Security

August 2020

By Derek S. Reveron and John E. Savage

Derek S. Reveron is Professor and Chair of the National Security Affairs Department at the U.S. Naval War College and Faculty Affiliate at the Belfer Center for Science and International Affairs at Harvard's Kennedy School of Government.
John E. Savage is the An Wang Professor Emeritus of Computer Science at Brown University and a Professorial Fellow at the EastWest Institute.

Abstract*: Over the past decade, people everywhere have become as dependent on the virtual world for their daily activities as they are dependent on the physical world for human activities. Global fiber optic networks have enabled communication in an unprecedented manner, connecting people in unique ways, propelling global supply chains, and giving consumers access to a variety of data from around the world. The online world is threatened by interstate rivals that engage in influence operations, economic espionage, and intelligence gathering and criminal groups that steal identities, ransom data, and grow their enterprises. Insiders facilitate intrusions wittingly and unwittingly raising the importance of corporations' roles in cybersecurity. This convergence between the virtual and physical worlds with the government and the corporate upends the entire frame of reference for national security, which is tilted toward physical attack and strict jurisdictional lines. As cybersecurity integrates further into U.S. national security, a new approach is needed to incorporate a human security construct at the user level. This article is adapted from their forthcoming book, Security in the Cyber Age from Georgetown University Press. The views expressed are their own.*

> *Rarely has something been so important and so talked about with less clarity and less apparent understanding [than information security]. . . . I have sat in very small group meetings in Washington . . . unable (along with my colleagues) to decide on a course of action because we lacked a clear picture of the long-term legal and policy implications of any decision we might make.*
>
> - General Michael Hayden, U.S. Air Force (retired), former head of the Central Intelligence Agency and the National Security Agency

General Michael Hayden's observation concerning information security helps illustrate why U.S. foreign policy is stifled by the Russian Federation's global influence operations, the People's Republic of China's global economic

doi: 10.1016/j.orbis.2020.08.005

espionage campaign, and digital human insecurity brought about by hackers, criminal groups, and intelligence services, all of which emerged gradually over time. By definition, slow-moving challenges are not crises, and it is hard to convene White House Situation Room meetings in the absence of the urgent. The system performs well in reaction to a major event, such as a terrorist attack or an invasion, but struggles when an issue is slow moving, such as expanding territorial claims, pandemic disease, climate change, or cyberinsecurity. This deficiency has as much to do with the scope of the challenge, but also illustrates a bias in U.S. national security processes and thinking where key actors are stuck in a Cold War paradigm—counting ships, creating military exercises for large-scale maneuver forces, and preparing for interstate conflict. The COVID-19 pandemic, which was predicted but unwanted and ignored, lays bare the national government's capabilities to address a virulent threat inside the country's borders and an inability to protect individual Americans' human security. This same orientation helps to explain the challenge to act when the nation is faced with incipient cybersecurity threats that individuals, organizations, and corporations face from foreign powers and organized crime.

General Michael Hayden

Admittedly, the prevailing international liberal order among states is being threatened as these words are written; great power politics are gaining attention again with China's hegemonic rise in East Asia, Russia's re-litigation of the Cold War's end, and U.S. efforts to re-trench and place America first. Yet, the United States is well-positioned for a world characterized by great power competition. In spite of decades of counterterrorism and counterinsurgency, the military services never stopped developing advanced weapons, such as the F-35 joint strike fighter, the Ford-class aircraft carrier, and new classes of missiles. China and Russia have reduced U.S. conventional advantages in key areas, but research and development continue to replace (and upgrade) nuclear warheads and the air-, land-, and sea-based delivery

systems to preserve the nuclear triad through century's end. Personnel numbers today have been stable since Bill Clinton was the U.S. president, the Services are re-orienting training for conventional military operations, and the Defense Department is developing a force for great power competition through its existing structures. Budgetary cuts always loom and program mismanagement undermine force development, but the U.S. military is largely prepared for conventional war.

The United States has had a combatant command to address threats in the Indo-Pacific since 1947, threats in Europe since 1952, and threats in the Middle East since 1983.[1] But the United States only created a military command to address cyber threats in 2010, with its full elevation to combatant command status in 2018. Today, U.S. Cyber Command largely is focused on defending Department of Defense (DOD) networks, supporting other combatant commands through cyberspace operations planning, and protecting critical infrastructure with other federal departments and the private sector. The latter is an important departure for defense thinking, which largely provides defense through overseas activities, yet Cyber Command provides indications and warnings to the public and private sector partners through malware alerts.[2] Reinforced by intelligence assessments, polling in the United States places cyber-insecurity as a leading national security challenge and a pressing concern for citizens and policymakers alike that should be addressed.[3]

(Photo by U.S. Cyber Command Public Affairs)

[1] Derek S. Reveron, *Exporting Security: International Engagement, Security Cooperation, and the Changing Face of the US Military, 2nd ed.* (Washington, D.C.: Georgetown University Press, 2016).

[2] "Cyber Strategy," Department of Defense, 2018, https://media.defense.gov/2018/Sep/18/2002041658/-1/1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[3] Dina Smeltz, Ivo Daalder, Karl Friedhoff, Craig Krafura, and Brendan Helm, "Rejecting Retreat: Americans Support US Engagement in Global Affairs," Chicago Council, 2019, see appendix fig. 3, https://www.thechicagocouncil.org/sites/default/files/report_ccs19_rejecting-retreat_20190909.pdf.

Recently, the National Security Agency (NSA) and Cyber Command have taken steps to help elevate the general level of cybersecurity globally. In January 2016, Rob Joyce, then-Chief of the NSA's Tailored Access Operations department, a group that does nation-state exploitation, gave a public talk at the USENIX Enigma conference in which he offered advice on how to defend against exploiters like his team.[4] In 2017, NSA published on GitHub, an open-source repository, some of its older technology, such as Security Enhanced Linux (SELinux).[5] In November 2018, the Cyber National Mission Force (CNMF), a subordinate unit of Cyber Command, created an account on VirusTotal, an online scanning service, and announced that it would share malware samples that it discovered on DoD networks. It also created a Twitter account (@CNMF_VirusAlert) to announce its postings to VirusTotal.[6] In 2019, again on GitHub, the NSA released Ghidra, a powerful cybersecurity tool for software reverse engineering. Ghidra converts binary code, bit strings readable by computers but not humans, into human-readable instructions. It is used for analyzing software, such as malware.[7] The unprecedented public release of such tools constitutes a trend for NSA and Cyber Command to work directly with code developers and commercial enterprises rather than focus exclusively on its intelligence mission and supporting military plans and operations.

Implicit in NSA's and Cyber Command's actions is the notion that cybersecurity addresses human security since it is individuals who are vulnerable and need defending. NSA has extended its remit beyond great power competition and now helps to protect national security at the user level. This is important since U.S. territory and population have been largely immune from physical conflict that happens outside the Western Hemisphere—cyber tools change this. Cyberspace operations give countries threatened by the United States the means to retaliate while largely avoiding escalation to the use of force.[8] Iran has already retaliated against the United States through cyber-attacks on the banking system, North Korea hacked the entertainment sector, China has stolen vast amounts of intellectual property and joined Russia in targeting the U.S. population through influence operations. In every case, the impact was felt by U.S. companies, organizations, and individual citizens (not military targets or the federal government). The cumulative effect undermines national security, yet

[4] "NSA TAO Chief on Disrupting Nation State Hacker," USENIX Enigma 2016, YouTube, https://www.youtube.com/watch?v=bDJb8WOJYdA.

[5] Tajha Chappellet-Lanier, "The NSA is now sharing a bunch of code on GitHub," fedscoop, June 22, 2017, https://www.fedscoop.com/nsa-now-sharing-bunch-code-github/.

[6] Catalin Cimpanu, "US Cyber Command starts uploading foreign APT malware to VirusTotal: USCYBERCOM said it plans to regularly upload 'unclassified malware samples' to VirusTotal," ZDNet, Nov. 8, 2018, https://www.zdnet.com/article/us-cyber-command-starts-uploading-foreign-apt-malware-to-virustotal/.

[7] Lily Hay Newman, "The NSA Makes Ghidra, a Powerful Cybersecurity Tool, Open Source," *Wired*, March 5, 2019, https://www.wired.com/story/nsa-ghidra-open-source-tool/.

[8] Benjamin Jensen and Brandon Valeriano, "What Do We Know about Cyber Escalation? Observations from Simulations and Surveys," Atlantic Council, Nov. 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf.

the national system largely ignored until recently since it was focused on cyber Pearl Harbors and cyber 9/11s. While there have been important changes in cybersecurity thinking, the convergence of the social with the digital creates a dilemma for U.S. national security. The question that the national security establishment must answer is: How and when to protect Americans in cyberspace from foreign intelligence services and foreign cyber commands? Examining cybersecurity through a human security lens can be instructive since the domestic/international and public/private divides disappear in cyberspace.

Human Security Goes Digital

Human security is largely absent from national security thinking and is often considered a soft issue left internationally for the Agency for International Development (AID) and non-governmental organizations (NGOs) or left domestically for state governments that provide education, regulate health care, subsidize it for those in need, and promote job creation. Defined as "a people-centered approach focused on individual human beings and their rights and needs," human security shifts focus from states to individuals and from tools of statecraft to conditions for social-economic development. It is based not in the United Nations Charter that privileges sovereignty of states, but in the Universal Declaration of Human Rights that exalts individuals.[9]

The United Nations Commission on Human Security best captures the meaning of human security: "Freedom from fear, freedom from want, freedom to live in dignity."[10] As the United Nations Development Program has phrased it, "Security is a child who did not die, a disease that did not spread, a job that was not cut, an ethnic tension that did not explode in violence, a dissident who was not silenced."[11] While national security and human security are often separated in the United States, national security cannot be achieved without first achieving human security. An educated population is essential to developing advanced military capabilities; a healthy population provides personnel to fill military ranks; and a robust economy provides tax revenue to fund activities and innovations to operationalize for the defense sector.

Challenges to human security include issues such as: climate change, pandemic diseases, endemic poverty, weak and failing states, transnational narcotics trafficking and criminal gangs, and vulnerable information systems. Given how closely tied human security is to development policies, human security is rarely mentioned in developed countries when discussing poverty, inadequate health care and education, and identity. However, if the term is broadened beyond a developing country context, then it can

[9] Derek S. Reveron and Kathleen A. Mahoney-Norris, *Human and National Security: Understanding Transnational Challenges* (New York: Routledge, 2019), p. 10.
[10] "Our Challenges are Shared; So, Too, is our Commitment to Enhance Freedom from Fear, Freedom from Want, Freedom to Live in Dignity' Says Secretary-General," United Nations, May 20, 2010, https://www.un.org/press/en/2010/ga10942.doc.htm.
[11] *Human Development Report 1994,* United Nations Development Program, http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf.

provide important insights into challenges faced by individuals in developed countries because it places focus on conditions that undermine citizens rather than sovereign states. As an example of human insecurity, COVID-19 unfortunately illustrates the impact on society and the economy.

In the information environment, human security is challenged by both states and nonstate actors. *Insiders facilitate intrusions wittingly and unwittingly, raising the importance of corporations' roles in cybersecurity.* Livelihoods are challenged by malicious code and intellectual property theft; and freedoms are challenged through surveillance and content manipulation. The connection at first may seem tenuous, but consider how the language of a human security issue such as health security is readily employed within the cybersecurity discourse: viruses and infections characterize the threats; vaccines (patches) and cyber-hygiene characterize the cure. Further, traditional national security concepts such as deterrence have been found inadequate to improve cybersecurity.

Conceptualizing cybersecurity as digital human security "prioritizes the individual, and views networks as part of the essential foundation for the modern exercise of human rights."[12] In general, countries, including the United States, see existing international law applicable to cyberspace, and 180 governments reaffirmed the applicability of the Universal Declaration of Human Rights online.[13] The European Union (EU) went further and implemented the General Data Protection Regulation (GDPR) on May 25, 2018. The three guiding principles of GDPR are: the protection of fundamental privacy rights for individuals, promotion of transparency in the ways that companies process data, and the free movement of data. The first two principles reflect European human rights laws where individuals retain ownership of their data, whereas the third principle is a rebuttal of data localization attempts. This inspired a California law that went into effect in 2020, which gave Californians greater privacy protections than those enjoyed by residents of the rest of the country and its territories. By conceptualizing cybersecurity through a human security lens, considerations of its impact on populations are made more visible and seen as more important for government to address.[14]

Unfortunately, the federal government's feeble response to COVID-19 mirrors its response to the cybersecurity threats created by ransomware, intellectual property theft, and identity theft. And in some cases, just like the COVID-19 response, individual states and cities are creating their own cybersecurity organizations to protect their citizens, but are limited given the global scope of the problem. To adequately address cyberspace insecurity, approaches need to include the panoply of actors that incorporate ideas from multiple academic disciplines.

[12] Ronald J. Deibert, "Toward a Human-Centric Approach to Cybersecurity," *Ethics & International Affairs*, vol. 32, no. 4 (Winter, 2018), pp. 411-424.
[13] Gabor Rona and Lauren Aarons, "State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace," *Journal of National Security Law & Policy*, vol. 8, no. 3, (2016), pp. 1-33.
[14] Gerald Zojer, "The Interconnectedness of Digitalisation and Human Security in the European High North: Cybersecurity Conceptualised through the Human Security Lens," *The Yearbook of Polar Law Online,* vol. 10, no. 1, 2019. pp. 297-320.

Scope of Digital Human Security

Like the physical environment, the information environment is all-encompassing and is bigger than hardware such as networks, telecommunication lines, and machines and the information that travels through the network such as data and media. Chinese and Russian influence operations highlight the importance of the cognitive realm or how people comprehend their experiences challenging the meaning of truth. When aggregated, cyberspace serves as a fifth dimension, where people can exist through alternate personae on blogs, social networking sites, and virtual reality games. Larry Johnson, chief executive officer of the New Media Consortium, predicts that we will experience the virtual world as an extension of the real one. Johnson writes:

> Virtual worlds are already bridging borders across the globe to bring people of many cultures and languages together in ways very nearly as rich as face-to-face interactions; they are already allowing the visualization of ideas and concepts in three dimensions that is leading to new insights and deeper learning; and they are already allowing people to work, learn, conduct business, shop, and interact in ways that promise to redefine how we think about these activities—and even what we regard as possible.[15]

Global fiber optic networks have enabled communication in an unprecedented manner, connecting people in unique ways, propelling global supply chains, and giving consumers access to a variety of data from around the planet. At the start of this decade, more than half of the world's population used the Internet on a regular basis.[16] This interconnection of the world's population within and across societies holds tremendous implications for economic growth and development, particularly for impoverished areas. It also gives countries the potential to overcome the challenges of being land-locked or geographically isolated from the developed core countries in North America, Europe, and East Asia. Space-based Internet will further connect the previously disconnected; interconnecting societies at the individual level has important benefits for every person, organization, commercial enterprise, and government. Unfortunately, national security tends to gaze beyond the water's edge and does not much consider how Americans are directly affected by cyberspace insecurity.

[15] Larry Johnson, "Thru the Looking Glass: Why Virtual Worlds Matter, Where They Are Heading, and Why We Are All Here," Keynote Address to the Federal Consortium on Virtual Worlds, Washington, D.C., April 24, 2008.
[16] "Usage and Population Statistics," Internet World Stats, http://www.internetworldstats.com/stats.htm.

Convergence of Physical and Digital Worlds

Within just the past decade, people everywhere have become almost as dependent on the digital world for their daily activities as they are dependent on the physical world. UN Secretary General António Guterres sees information technology as socially transforming and as integral to human security since "farmers can monitor prices, refugees can let their families know they are safe, and health workers can check a patient's status or respond to emergencies."[17] In other words, cybersecurity is intertwined with human security.

Global communications are now commonplace, vast amounts of knowledge are at our fingertips, enormous amounts of computational power are readily available, and artificial intelligence has become a reality, creating new opportunities for businesses and new types of work. The great illustration of this powerful medium has occurred in 2020 during the COVID-19 pandemic. Hundreds of millions of workers shifted to telework during quarantines caused by a global pandemic; schools shifted to remote learning; and individuals remained connected while practicing social distancing making self-isolation bearable.

As new technologies come online, they represent significant promise for deepening society's connections in cyberspace. Improving encryption technology will deepen the personal and the digital; 5G wireless communication with its potential for very high data rates will revolutionize mobile platforms; the technologists promise that autonomous vehicles will proliferate in a secure, high-speed environment. These are exciting times, but each new breakthrough seems to create unintended vulnerabilities that undermine cybersecurity with societal-level impacts that individuals experience at the human security level.

These impacts can range from the inconvenient, such as stopping payment systems at a major retail corporation, to the existential, such as terminating power for a city in the middle of a cold winter. Lacking an adequate cybersecurity framework, policymakers see cyber exploits as threats often generating fear, uncertainty, and doubt in the information technology sector rather than a public safety concern for government. The challenge for humanity is to master the technologies of cyberspace and control their misuses so that their full potential can be realized. Because cyberspace is ubiquitous, cybersecurity must be a universal concern. To paraphrase Bruce Schneier, computer security has become everything security.[18] This means government must be more active in cybersecurity to use its ability to convene stakeholders, regulate information and technology products like it does with other consumer products, and protect the marketplace from products that undermine user's security.

[17] "Fast Forward Progress: Leveraging Tech to Achieve the Global Goals," quoted in United Nations, http://www.itu.int/en/sustainable-world/Documents/Fast-forward_progress_report_414709%20FINAL.pdf.

[18] Kat Hall, "Infosec guru Schneier: Govts will intervene to regulate Internet of Sh!t," *The Register*, June 8, 2017, https://www.theregister.co.uk/2017/06/08/governments_will_intervene_insecure_iot/.

Elevating Digital Human Security

Broadly speaking, intra-state, transnational, and regional actors challenge a sovereign government's ability to provide a secure environment for its citizens. This is true on land, air, sea, space, and cyberspace. Yet, unlike other challenges, such as economic development, terrorism, or border disputes, where governments have well-established procedures for addressing conflicts or malicious activity, the same is not true in cyberspace. Government is either absent or follows information and communications technology (ICT) companies that pursue global business models rather than national interests. The gap between threats and government responses generate security deficits, which are evidenced through regular reports of cyberspace insecurity. By focusing on traditional security concerns, governments do not address how cyberspace insecurity undermines their populations. Thus, for many in the United States and citizens of other developed countries, the ultimate threat to their individual human security comes from cyberspace.[19]

Digital human security is not just a personal issue, but is of increasing salience on the national security agenda. Former U.S. Director of National Intelligence Dennis Blair testified to this point: "The growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructure."[20] This disruption became real when Russia conducted a cyberattack against a Ukrainian power plant in December 2015, which denied power to about 200,000 Ukrainians.[21] Though it had a temporary effect, the attack was a harbinger; civilians at scale are vulnerable to geopolitical tensions. The Trump administration's first Director of National Intelligence Dan Coats extended the ideas linking cybersecurity to a human security construct: "Cyber threats also pose an increasing risk to public health, safety, and prosperity as cyber technologies are integrated with critical infrastructure in key sectors."[22] This convergence creates challenges as the world addresses the impact of the pandemic caused by COVID-19. Plans to enable digital health certificates to facilitate the movement of people can be jeopardized by corrupting health records. Efforts to use contact tracing to monitor infection spread can be harnessed to analyze social networks denying freedom of assembly. Intellectual property theft of pharmacological data undermines global

[19] See, Derek S. Reveron, ed., *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Washington, D.C.: Georgetown University Press, 2012).
[20] Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee: Statement for the Record*, March 10, 2009, pp. 39–40.
[21] Kim Zetter, "Inside the Cunning, Unprecedented Cyber Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
[22] Daniel R. Coats, "Statement for the Record Worldwide Threat Assessment of the U.S. Intelligence Community Senate Armed Services Committee," May 23, 2017, https://www.dni.gov/files/documents/Newsroom/Testimonies/SASC%202017%20ATA%20SFR%20-%20FINAL.PDF.

cooperation with the potential to create counterfeit vaccines that have not been fully tested.

As more of society, government, and the economy move online, individuals in developed countries can no longer be isolated from the effects of war. Americans have become accustomed to seeing their military fight wars abroad with little impact on the homeland; cyberspace attacks have the potential to change this perception. Adversaries may disrupt Americans' access to such fundamental necessities as electricity, telecommunications, and water. Initial cybersecurity efforts focused on protecting technical infrastructure from attacks against industrial control systems, but since 2016, foreign powers' activities through social media have preoccupied U.S. intelligence. This was in response to foreign powers' influence operations that shape U.S. voters' views and undermine democracy.[23] As Stanford's Hoover Institute Senior Research Fellow Herb Lin wrote, "Cyberattacks are particularly well suited for attacks on the psychology of adversary decision makers who rely on the affected computers, and in this case such effects can be regarded as indirect effects."[24] Consequently, the Executive Branch developed plans to protect the election system to include creating a Foreign Influence Task Force. Congress also considered ways to regulate social media without undermining free speech and ways to protect infrastructure with respect to global supply chains. ICT corporations have also become more active to protect their platforms from misuse while adhering to their corporate vision. In spite of these efforts, William R. Evanina, the director of the National Counterintelligence and Security Center, noted just months before the 2020 presidential election, "foreign states will continue to use covert and overt influence measures in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic process."[25]

The Case of China

Threats to digital human security are not only technical with the ability to steal intellectual property or shutdown industrial systems as discussed, but also cognitive given the great power competition between the United States and China. Author Jon Lindsay has written, "A distinguishing characteristic of the Chinese concept of

[23] Nikki Floris, "Securing America's Elections: Oversight of Government Agencies. Statement before the House Judiciary Committee," Oct. 22, 2019, https://www.fbi.gov/news/testimony/securing-americas-elections-oversight-of-government-agencies-102219.

[24] Herb Lin, "Operational Considerations in Cyber Attack and Cyber Exploitation," in Derek S. Reveron, ed., *Cyberspace and National Security,* p. 41.

[25] "Statement by NCSC Director William Evanina: Election Threat Update for the American Public," Office of the Director of National Intelligence, Aug. 7, 2020, https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

information security (xinxi anquan) is that it emphasizes Internet content as much as, if nor more than, technical network security (wangluo anquan)."[26] This statement is a reflection of China's political culture that promotes the collective good over individualism. The Chinese Communist Party (CCP) relies on this cultural representation to reinforce its political monopoly in China. Then-Director of the Information Office of the State Council and the External Propaganda Department of the CCP Wang Chen explained:

> These problems [harmful language, obscenities, and leaks] have restricted the healthy and sustainable development of the Internet and affecting the overall situation of our reform and development. We must pay special attention to resolving these problems.[27]

The Chinese government uses aggressive content moderation to eliminate objectionable political speech, but also to promote a particular political agenda. For example, in the wake of the 2020 COVID-19 outbreak that originated in Wuhan, China, the main messaging app WeChat used blacklisted keywords to remove content (e.g., coronavirus and Wuhan seafood market) between senders and recipients.[28] This ability is an authoritarian's dream in that a government can now change text messages while in transit to limit information flow among individuals enabling the government to control the narrative. Further, the Cyberspace Administration of China told technology companies "that it would punish 'websites, platforms, and accounts' for publishing 'harmful' content and 'spreading fear' related to COVID-19."[29] This warning had global implications by creating delays in how other governments responded to the pandemic.

Additionally, the CCP uses content moderation and cyber means to target political opponents inside China and around the world. Then-Senior Researcher at the Citizen Lab Sarah McKune has written, "Efforts to control Tibetans have ramped up in the digital realm, which is perceived as a primary conduit for hostile foreign influence."[30] Similar efforts are made against religious groups, such as Falun Gong, pro-Taiwan independence groups, and other ethnic minorities, such as Uyghurs.

[26] Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Doman* (New York: Oxford University Press, 2015), p. 11.
[27] Wang Chen, "Concerning the Development and Administration of Our Country's Internet," in Human Rights in China, tr., *China Rights Forum: "China's Internet": Staking Digital Ground,* no. 2 (2020), https://www.hrichina.org/en/content/3241.
[28] Lotus Ruan, Jeffrey Knockel, and Masashi Crete-Nishihata, "Censored Contagion How Information on the Coronavirus is Managed on Chinese Social Media," Citizen Lab, March 3, 2020, https://citizenlab.ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media/.
[29] Ruan, Knockel, and Crete-Nishihata, "Censored Contagion," March 3, 2020.
[30] Sarah McKune, "'Foreign Hostile Forces': The Human Rights Dimension of China's Cyber Campaigns," in Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, eds., *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (New York: Oxford University Press, 2015), p. 274.

Senior Lecturer at James Cook University Anna Hayes, for example, has argued that "Xi [Jinping] has overseen a hard-line approach towards Xinjiang and the Uyghurs, increasing surveillance and policing to unprecedented levels."[31] By transforming Xinjiang into a surveillance state, Beijing seeks to control Uyghurs in both cyberspace and physical space, thereby undermining digital human security and basic human rights.

U.S. Strategic Thinking

The bias toward protecting against physical infrastructure attack from cyber-9/11s, rather than digital human security, is rooted in U.S. strategic thinking. Cybersecurity first emerged as a distinct national security policy area in 1998 when President Bill Clinton signed Presidential Decision Directive 63, which established a White House structure to coordinate government and private action to "eliminate any significant vulnerability to both physical and cyberattacks on our critical infrastructures, including especially our cyber systems."[32] To establish redlines against such attacks, President George W. Bush declared in 2003 that it would be the "policy of the United States to protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States."[33]

Both administrations emphasized the catastrophic scenarios of cyber Pearl Harbor and a cyber 9/11-style attack reflecting traditional national security thinking through defense strategies. The March 2005 *National Defense Strategy* identified cyberspace as a new theater of operations and assessed cyberspace operations as a potentially disruptive challenge, concluding that in "rare instances, revolutionary technology and associated military innovation can fundamentally alter long-established concepts of warfare." The 2008 *National Defense Strategy* explored these implications further, assessing that small groups or individuals "can attack vulnerable points in cyberspace and disrupt commerce and daily life in the United States, causing economic damage, compromising sensitive information and materials, and interrupting critical services such as power and information networks."[34]

Despite recognized vulnerabilities and threats to cyberspace, there are clear gaps in the way that policy and law address these concerns. International law and national security policy identify intrusions as sovereignty violations, but policymakers struggle with how to respond to cyber operations. The North Atlantic Treaty Organization (NATO) has identified cyberspace as a domain of operations, and

[31] Anna Hayes, "Interwoven 'Destinies': The Significance of Xinjiang to the China Dream, the Belt and Road Initiative, and the Xi Jinping Legacy," *Journal of Contemporary China*, vol. 29, no. 121 (2020), pp. 31-45.
[32] "Critical Infrastructure Protection," sec. 2, Presidential Decision Directive 63, White House, May 22, 1998, https://fas.org/irp/offdocs/pdd/pdd-63.htm.
[33] *The National Strategy to Secure Cyberspace*, White House, 2003. https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.
[34] Secretary of Defense, *National Defense Strategy*; Department of Defense, (2008), p. 7. https://archive.defense.gov/pubs/2008NationalDefenseStrategy.pdf.

offensive cyberspace operations could be interpreted in the context of collective self-defense through Article 5, but it seems unlikely that the Alliance would risk escalation with Russia. International Legal Scholar Michael Schmitt has argued that cyberspace is far from the wild west, but there is ambiguity in application of international law "exacerbated by the practice of some states to 'cherry-pick' amongst the international law rules that govern cyberspace."[35]

After wading through the meaning of Iran's distributed denial of service attacks on the U.S. financial sector in 2012-2013, North Korea's compromise of Sony Entertainment in 2014, China's decades-long economic espionage against U.S. corporations, and Russia's influence operations in 2015-2016, strategic thinking looked beyond deterrence. *New York Times* National Security Correspondent David Sanger captured the sentiments of the Obama administration in its final days by writing that "in the cyber age, we have not found that balance [of power] and probably never will . . . it amounts to an admission that our defenses at home are wildly insufficient and that the only way to win is to respond to every perceived threat."[36] As a consequence, the United States promoted a policy of "persistent engagement" and "defend forward." As defined by United States Military Academy Professor Erica Borghard for the Cyberspace Solarium Commission, defend forward "entails the proactive observing, pursuing, and countering of adversary operations and imposing costs in day-to-day competition to disrupt and defeat ongoing malicious adversary cyber campaigns, deter future campaigns, and reinforce favorable international norms of behavior, using all instruments of national power."[37]

According to the Head of U.S. Cyber Command General Paul Nakasone, "This persistence force will contest our adversaries' efforts in cyberspace to harm Americans and American interests. It will degrade the infrastructure and other resources that enable our adversaries to fight in cyberspace."[38] U.S. government policy continues to evolve as it copes with tension between corporations that want to prevent governmental disruption of commercial activity and the Executive Branch that seeks greater authority to provide security in cyberspace. The 2018 White House national cyber strategy noted, "Economic security is inherently tied to our national security," so close public-private collaboration is a cornerstone of U.S. cyber strategy.[39] That

[35] Michael N. Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law Rules for Cyberspace," *Texas National Security Review,* Summer 2020, https://tnsr.org/2020/07/taming-the-lawless-void-tracking-the-evolution-of-international-law-rules-for-cyberspace/.

[36] David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018), pp. 296, 301

[37] Erica Borghard, "Operationalizing Defend Forward: How the Concept Works to Change Adversary Behavior," *Lawfare*, March 12, 2020, https://www.lawfareblog.com/operationalizing-defend-forward-how-concept-works-change-adversary-behavior .

[38] Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly*, vol. 92, Feb 2019, p. 11, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.

[39] "National Cyber Strategy of the United States of America," White House, Sept. 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

same year, Congress created the Cybersecurity and Infrastructure Security Agency (CISA) overseen by the Department of Homeland Security (DHS). CISA grew out of the National Protection and Programs Directorate at DHS and serves as an important coordinating function within the national government. DHS' distance from the National Security Agency does emphasize the civilian dimension of cyberspace, which is important to promote public-private cooperation. Additionally, the National Cyber Investigative Joint Task Force (NCIJTF) is focused on pursuing those who violate U.S. cybersecurity laws. Internationally, the U.S. and its allies have raised the alarm on the threats posed by Chinese technology companies and is using the Committee on Foreign Investment in the U.S. (CFIUS) process more aggressively.

Cyber and the Policy Process

Using cyberspace capabilities as a tool of power poses a number of challenges for the national security process. While cyber is a relatively new tool, former Department of State (DOS) Counselor Philip Zelikow argues that its uses are rooted in a broader context with

> a record of policy failures: the tendency to react to events rather than drive them, poorly specified objectives, confusing guidance, reliance on weakly evidenced suppositions, little grasp of organizational capacities, inability to adapt organizations to new problems, overreliance on ill-managed contractors. These are all symptoms. They are symptoms of policies that are badly designed.[40]

As the U.S. government further integrates cyberspace capabilities in developing strategic options, new ways of thinking are necessary since cyberspace upends the entire frame of reference by challenging domestic and foreign boundaries that we use to create authorities for national security. As conceived, the Internet is a borderless network, so cybersecurity is global. To be sure, the telecommunications lines cross borders, but data move seamlessly. Unlike people crossing borders, no passports or visas are required; unlike mail, no customs agreements and inspections are required. To be sure, some countries that are unhappy with an uncontrolled cyberspace are regulating traffic and using sensors and gateways to alter the open cyberspace landscape, but overall Internet architecture is designed to transcend sovereignty.

The open nature of cyberspace creates particular legal and organizational challenges for countries that have sharp divisions between domestic and international security. For example, in the United States, the Federal Bureau of Investigation (FBI), within the Department of Justice (DOJ), has jurisdiction for domestic surveillance and law enforcement, whereas the National Security Agency (NSA), within the DOD, has jurisdiction for external surveillance. The director of NSA also leads U.S. Cyber

[40] Philip Zelikow, "To Regain Policy Competence: The Software of American Public Problem-Solving," *Texas National Security Review*, vol. 2, no. 4, Sept. 2019, https://tnsr.org/2019/09/to-regain-policy-competence-the-software-of-american-public-problem-solving/#_ftnref16.

Command, which is responsible for external cyber operations in support of military campaigns. And the Department of Homeland Security's CISA works across government and the private sector to secure critical infrastructure. Each organization has separate legal authorities and cultures that can complicate coordination. This is exacerbated by the different committees and sub-committees that provide congressional oversight.

Reconciling these different organizational perspectives in policy discussions exemplifies Government Administrator Rufus Miles' adage from the late 1940s, "Where you stand, depends on where you sit."[41] Encryption is illustrative. The National Security Agency collects foreign intelligence, so it wants to limit encryption to ensure it can read intercepted communications. The DOS has an Internet freedom agenda, so it thinks encryption is essential for civil society in authoritarian countries. The Department of Commerce wants to promote U.S. standards as global ones, so it looks to be inclusive to promote investment and U.S. business. And the Treasury Department's CFIUS process looks at investments in U.S. business and real estate with concern for national security. This challenge is similar to non-cyber policy; efforts over the last two decades to reform the interagency process and establish whole-of-government policies, which does not bode well for the future of cybersecurity.

Cybersecurity also challenges public-private responsibility for security. Unlike traditional domains, such as airspace, land borders, and maritime boundaries, that are controlled and monitored by a national government, cyberspace is created and monitored largely by private companies; operating systems, hardware, and telecommunication lines are corporate and private, but not governmental. Corporations are not simply selling weapons and services to the DOD; they are also active players in cyberspace. For example, Microsoft is promoting international norms for all governments, Facebook is countering misinformation and inauthentic postings globally, and Twitter is closing terrorists' feeds. In other words, cybersecurity, unlike missile defense, is not the exclusive domain of government. Corporations create and maintain cyberspace. Many are also lobbying government on questions of privacy, encryption, and vulnerability disclosure. Corporations establish the terms of use and the relationship with its users. Finally, the existing national security system divides responsibilities further between the national government and state governments. The U.S. system of federalism can have the effect of muting the federal government's role in domestic security, which is largely in the hands of state governments and cities. This has resulted in states and cities developing their own cyber task forces and commissions creating another coordination dimension to share data to improve cybersecurity.

[41] Rufus E. Miles, "The Origin and Meaning of Miles' Law," *Public Administration Review,* vol. 38, no. 5 (1978), pp. 399-403.

The Future of Cyberspace

Since the Advanced Research Projects Agency Network's (ARPANET's) humble beginnings in 1969, governments have been moving past laissez-faire approaches to the information technology sector and using national and international institutions and practices to increase their involvement in cyberspace. A country's political system and regime type are driving domestic regulation to turn away from the original version of the Internet, where users can be anonymous, and borders are meaningless when connecting people to people. The EU is at the forefront of extending human rights in cyberspace, while China has taken the lead in undermining human security through digital repression. The different approaches reflect their political cultures rather than the nature of technology. With dozens of countries that are developing cyber commands, it seems fair to conclude that cybersecurity concerns have gained currency in national security circles, but the focus must shift from interstate rivalry, preoccupied with conventional warfighting, to more nuanced thinking about security that examines how great power competition affects individuals and corporations that produce and maintain much of cyberspace.

Barring some cataclysmic event, information and communications technology is the latest tool that humans developed that will have widespread impact on economic and social development. Just like other tools, information technology holds both the promise of a better future and the prospect for increasing misery unless digital divides narrow, and people adapt to new economic realities brought about by technological change. The same is true when thinking about cybersecurity as national security. As Atlantic Council Senior Fellow Kenneth Geers reminds us, "[The] Internet today is merely a reflection of what came before—including crime, espionage, and warfare—and the international security environment is still closer to Pandemonium."[42]

There are concerted efforts to reduce the pandemonium through domestic regulation, international norms, law, and institutions, and ethics in technology. While we interface through a screen, our language is translated into bits, and ideas are transmitted through data packets, we must remember that the Internet is simultaneously a commercial, social, and sovereign space. Better programming, better encryption, and artificial intelligence will take the security cat-and-mouse game to a higher level, but the answer lies just as much in human behavior and requires serious work to improve digital human security. Users must be active participants in efforts to improve cybersecurity.

Undoubtedly, there is much uncertainty about the future of cybersecurity. The uncertainty is based on technological change, but also on how society integrates new technologies into political, social, economic, and national security practices. The Internet is no longer a luxury, but a digital necessity to participate in society. It increasingly demands government attention to make cyberspace safer and more secure by promoting digital human security.

[42] Kenneth Geers, "Cyber Weapons Convention," *Computer Law and Security Review,* vol. 26, no. 5 (2010), pp. 547-551.