United States International Cyberspace & Digital Policy Strategy

Towards an Innovative, Secure, and Rights-Respecting Digital Future

TABLE OF CONTENTS

Preface

We are in a pivotal period of international relations, characterized by acute competition between nations, and shared global challenges like climate change, food and health security, and inclusive economic growth.

Technology will play an increasingly critical role in addressing these challenges. That is why at the State Department we have prioritized building capacity and expertise in cyber, digital, and emerging technology issues as part of our broader efforts to modernize diplomacy and ensure U.S. foreign policy delivers on the issues that matter most to the lives and livelihoods of the American people. As a key milestone in this work, I am pleased to share here the Department's International Cyberspace and Digital Policy Strategy.

Central to our strategy is the effort to build digital solidarity – working together to offer mutual assistance to the victims of malicious cyber activity and other digital harms; assist partners – especially emerging economies – in deploying safe, secure, resilient, and sustainable technologies to advance their development goals; and builds strong and inclusive innovation economies that can shape our economic and technological future. We are rallying coalitions of governments, businesses, and civil society to shape the digital revolution at every level of the technology "stack" – from building subsea cables and telecommunication networks, to deploying cloud services and trustworthy artificial intelligence, to promoting rights-respecting data governance and norms of responsible state behavior.

The United States will work with any country or actor that is committed to developing and deploying technology that is open, safe, and secure, that promotes inclusive growth, that fosters resilient and democratic societies, and that empowers all people.

Antony J. Blinken
Secretary of State

Introduction

The United States seeks to work with allies, partners, and stakeholders across the globe to shape the design, development, governance, and use of cyberspace and digital technologies to advance economic prosperity and inclusion; enhance security and combat cybercrime; promote and protect the exercise of human rights, democracy, and the rule of the law; and address transnational challenges. The United States believes in the critical role that the responsible uses of digital technologies and interconnected networks play in empowering people, and that an open, interoperable, secure, and reliable Internet enables new solutions to global challenges. Autocratic states and other actors, however, have used cyber and digital tools to threaten international peace and stability, harm others, exert malign influence, and undermine the exercise of human rights. An innovative, rights-respecting international cyberspace and digital technology policy strategy is foundational to U.S. strategic, security, economic, and foreign policy interests.

Leadership in cyberspace, the digital economy, and emerging digital technologies is central to advancing the U.S. vision set forth in the October 2022 National Security Strategy (NSS) of a "free, open, secure, and prosperous world." As the lead foreign policy agency for the United States, the Department of State is advancing the 2023 National Cybersecurity Strategy (NCS) and its objectives of forging international partnerships to build an open, resilient, defensible, and rights-respecting digital ecosystem. It is also strengthening the Strategy's dual approach of 1) rebalancing responsibility for defending cyberspace onto the government and private sector organizations that are the most capable and best positioned to reduce risks and of 2) realigning incentives to favor long term investment in cybersecurity through diplomacy, partnerships, and information-sharing. This strategy will be complemented by the U.S. Agency for International Development's (USAID) forthcoming Digital Policy.

To advance the NSS and NCS, the Department of State, working with other federal agencies, has developed an international cyberspace and digital policy strategy focused on building broad digital solidarity through three guiding principles and four areas of action to be prioritized over the next three to five years.

Digital solidarity is a willingness to work together on shared goals, to help partners build capacity, and to provide mutual support.[1] Digital solidarity recognizes that all who use digital technologies in a rights-respecting manner are more secure, resilient, self-determining, and prosperous when we work together to shape the international environment and innovate at the technological edge. Central to the tenets of digital solidarity are efforts to support allies and partners, especially emerging economies, to fully seize the opportunities presented by new technologies and sustainably pursue their economic and development goals. Digital solidarity aligns U.S. national interests with those of our international partners through compatible approaches to technology governance, sustains strong partnerships with civil society and the private sector, and embraces cybersecurity resilience built on a diversity of products and services made by trusted technology vendors. It highlights the mutual support that the United States and its partners offer one another to counter and respond to malicious cyber operations, cybercrime, and other digital harms, and promotes cooperative efforts among states and civic actors to defend and advance human rights. In addition, the concept of digital solidarity rests on efforts to build digital and cyber capacity so that partners are not only better able to build a defensible and resilient digital ecosystem over the long term but are also able to respond and recover quickly when incidents that threaten security, safety, and rights happen. The actions and efforts of this strategy are intended to demonstrate and build digital solidarity with partners across the globe.

The Department of State, with interagency partners, will build digital solidarity through four areas of action, fundamentally supported by three principles:

First, the Department of State will pursue an affirmative vision for cyberspace and digital technologies focused on delivering the benefits of technology and grounded in international commitments and international law, including international human rights law. The United States is committed to working with allies and partners toward a future in which people around the world use digital technologies safely to seek, receive, and impart information and ideas online as they participate in free, open, and informed societies; access educational and economic opportunities in order to drive inclusive economic growth; and reliably receive critical services and information from their governments.

Second, the Department of State will integrate cybersecurity, sustainable development, and technological innovation throughout our approach. Cybersecurity, data security, and cyber-resilience are prerequisites for and enablers of economic growth and healthy civic spaces where citizens can exercise their rights; countries cannot build and support an innovative digital ecosystem that benefits everyone without first securing it.

in **Third**, the Department of State will implement a comprehensive policy approach that uses the appropriate tools of diplomacy and international statecraft across the entire digital ecosystem. This ecosystem includes but is not limited to hardware, software, protocols, technical standards, providers, operators, users, and supply chains spanning telecommunication networks, undersea cables, cloud computing, data centers, and satellite network infrastructure, operational technologies, applications, web platforms, and consumer technologies as well as Internet of Things (IoT), artificial intelligence (AI) and other critical and emerging technologies. **[2]**

In line with these three principles, the Department of State will build digital solidarity through four areas of action, which flow from creating and governing digital ecosystems to defending against malicious actions and delivering assistance and building resilience:

1. Promote, build, and maintain an open, inclusive, secure, and resilient digital ecosystem;

2. Align rights-respecting approaches to digital and data governance with international partners;

3. Advance responsible state behavior in cyberspace, and counter threats to cyberspace and critical infrastructure by building coalitions and engaging partners;

4. Strengthen and build international partner digital and cyber capacity.

The Department of State will reinforce efforts to forge digital solidarity by its proactive participation in international, multilateral, and multistakeholder bodies where obligations, norms, standards, and principles are developed that impact cyberspace, digital, Internet, and technology issues. While progress in these venues can be slow and incremental – frequently as a function of their objectives—but a lack of U.S. leadership in international fora may allow adversaries to fill the void and shape the future of technology to the detriment of U.S. interests and values.

Nearly all foreign policy issues – from international security to democracy and human rights to global health and climate change – will be shaped by today's investments in cyberspace and digital technology diplomacy. The Department of State will lead the interagency process to set, coordinate, and integrate cyber and digital technology diplomacy efforts to advance U.S. national interests and values over the next decade and beyond. The efficacy of U.S. efforts and related messaging, however, depends in part on consistency and action at home, both in policy and on execution. For example, U.S. technology companies are the leaders in the first wave of digitalization and are now pushing the innovative edge on AI systems. The United States, therefore, should be a leader in promoting accountability for technology

platforms. We need to help lead the responsible design, development, governance, and use of the next wave of technologies in line with democratic values and respect for human rights.

The United States has great strengths that serve us in shaping the future of digital technologies: strong alliances and partnerships; the world's most innovative technology companies; a transparent, inclusive, and enabling policy environment; and robust and engaged civil society and technical communities. The United States is mobilizing these resources to implement this affirmative and proactive international cyberspace and digital strategy.

The Digital World: Opportunities and Challenges

Figure 1. Abstract representation of a digital, connected world. (Adobe Stock photo.)

Digital technologies have revolutionized how we live, work, and learn. They, along with expanded connectivity, not only power economic growth but also facilitate the exercise of human rights and improve access to education, financial, and social services. Digital technologies have created new markets and opportunities and have enabled businesses to reach a vast customer base beyond their country's borders. New digital tools have energized civic and political engagement, democratized information and knowledge, been used to hold governments and companies accountable, and increased the transparency, efficiency, and responsiveness of public services.

Looking ahead, these technologies can unlock unparalleled opportunities to address some of the most pressing global challenges, including climate change, economic and social inequality, and health crises. By harnessing the power of data analytics, AI, and real-time connectivity, we can create smarter, more sustainable cities, improve agricultural yields using fewer resources, and make healthcare accessible to even the most remote communities. These technologies enable the development of green energy solutions, fostering a transition towards cleaner and less expensive energy. Advances in data collection, modeling, simulation, and analysis will allow scientists to accelerate research and discovery and identify patterns invisible to humans alone, catalyzing rapid and unexpected breakthroughs. By connecting people and information like never before, digital technologies can foster a more inclusive, equitable world where opportunities for prosperity and well-being are abundant for all.

At the same time, significant harms have accompanied the rapid expansion and evolution of digital technologies. The geopolitics of cyberspace are competitive and complex. Malicious state and non-state actors have developed the capabilities and demonstrated the intent to place critical infrastructure, national critical functions, and even individual citizens at risk. Authoritarian states are promoting competing forms of technology governance that use mass surveillance, privacy-invasive data collection practices, and online censorship tools that threaten the open, interoperable, secure, and reliable Internet. Technology provides new vectors and tools for crime, and the dramatic spread of personal information online has expanded the threat environment. The proliferation and misuse of commercial spyware is a threat to national security, targeting U.S. officials abroad; commercial spyware has also been used to, target and intimidate perceived opponents, facilitate efforts to curb dissent, and thus undermine democratic values. Journalists, activists, educators, researchers, women and girls, and marginalized groups are often the victims of unlawful surveillance, online harassment, and abuse. Countries and technology platforms each have a role to play in mitigating algorithmic bias and information manipulation, as well as violent extremist messaging, child sexual abuse material (CSAM), technology-facilitated gender-based violence, and other harmful content.

These challenges are pressing and high stakes. Innovation, partnerships, collaboration, coalition building, information sharing, mutual support, assistance, and the other tools of diplomacy are essential to ensuring that digital technologies defend and advance individual freedom and promote economic prosperity.

Cyber Attacks and National Security Threats

Adversarial cyber campaigns can cumulatively produce strategic loss for the United States and its allies, and they increasingly put the development goals of emerging economies at risk. Cyber threats continue to intensify in both frequency and severity, with increased risks of escalatory or uncontrolled cyber activity. State actor and non-state actors, including criminals, terrorists, and violent extremists, have tremendous incentives to invest in and exploit digital technologies to threaten our and other's national interests.

The People's Republic of China (PRC) presents the broadest, most active, and most persistent cyber threat to government and private sector networks in the United States. Beijing has mounted cyber espionage operations against government, commercial, and civil society actors and has increased its ability to carry out destructive and disruptive cyberattacks. The PRC is capable of launching cyberattacks that could disrupt oil and gas pipelines, rail systems, and other critical infrastructure services within the United States or its allies and partners. Attempts to compromise critical infrastructure by PRC actors are designed in part to pre-position themselves to be able to disrupt or destroy critical infrastructure in the event of a conflict—either to either prevent the United States from being able to project power into Asia, or to affect our decision-making during a crisis by instigating societal chaos inside the United States. Both state-sponsored activity and that of PRC-linked actors are part of the PRC cyber approach.

A persistent cyber threat, the Russian government is refining its cyber espionage, cyberattack, influence, and information manipulation capabilities to threaten other states and to weaken U.S. alliances and partnerships. Russia continues to provide safe haven to transnational cybercriminal actors, such as disruptive ransomware gangs. Russia's cyberattacks in support of its 2022 unprovoked invasion of Ukraine were intended to destabilize the Ukrainian state and military and have resulted in spillover effects onto civilian critical infrastructure in other European countries. As the war continues, Russian government and Russian government-aligned cyber actors have targeted Ukraine with cyber operations against the public and private sectors, information manipulation and online influence operations, and attempts to divert and censor Ukrainians' access to the Internet. Russia appears particularly focused on improving its ability to target critical infrastructure in the United States to demonstrate its ability to damage infrastructure during a crisis.

The governments of the Democratic People's Republic of North Korea (DPRK) and Iran have both increased the scale of their malicious cyber activities. Facing multiple rounds of international sanctions, the DPRK evades controls through cybercrime and the theft of cryptocurrencies. DPRK hackers continue to gather intelligence on military technology targets as well as academia and think tanks. In addition, the DPRK dispatches thousands of skilled IT workers around the world to generate fraudulent revenue that ultimately contributes to its weapons of mass destruction and ballistic missile programs despite U.S. and UN sanctions.

Iran's growing expertise and willingness to conduct cyber operations threaten the security of networks and data globally. Iran's opportunistic approach to cyberattacks makes critical infrastructure owners in the United States susceptible to being targeted by Iranian actors, particularly when Tehran believes that it must demonstrate it can push back against the United States in other domains. Iranian actors have engaged in a wide range of intelligence-gathering operations around the world, and—in the wake of Hamas' atrocities on October 7, 2023, and Israel's military operations in Gaza—have conducted wiper, website takedown, hack and leak operations, espionage, and online information manipulations campaigns. Iranian actors have also conducted malicious activity against operational technology devices used in the water sector and other industries.

Cyber criminals and criminal syndicates operating in cyberspace now represent a specific threat to the economic and national security of countries around the world. Cybercrime and online fraud cause significant harm to economic development, with small- to medium-sized enterprises and financial service providers especially at risk. According to one estimate, the global cost of cybercrime is estimated to top $23 trillion in 2027. **[3]**

Ransomware incidents have disrupted critical functions, services, and businesses, from energy pipelines and food companies to schools and hospitals. Ransomware attacks against the healthcare industry can undercut the level of care provided to patients and others under care. Total economic losses from ransomware attacks worldwide continue to climb, reaching into the billions of U.S. dollars annually. Ransomware groups often operate out of safe haven jurisdictions whose governments, often adversaries like Russia, do not cooperate with law enforcement and sometimes encourage, direct, sanction, or tolerate their activities.

Terrorists' and violent extremists' use of digital technologies also represents a threat to the national security of the United States and its allies and partners. Malign activities include the use of information and communications technologies (ICT) to spread violent propaganda; encourage radicalization and mobilization to commit violent acts; recruit individuals to terrorist organizations; to train, plan, and coordinate attacks; and finance terrorist acts.

Competing Internet Norms

Russia, the PRC, and other authoritarian states have promoted a vision of global Internet governance that centers on domestic control and top-down, state-centric mechanisms over the existing bottom-up multistakeholder processes. Russia and the PRC attempt to use multilateral fora like the UN to exert their influence on and appeal to developing countries, with the aim of reshaping the global cyber and technology policy landscape to advance an authoritarian agenda while hampering the United States and its allies. Russia, the PRC, and others seek to reshape norms governing cyberspace, undermine the technical underpinnings of the Internet, and dilute accountability for authoritarian countries' malicious use of cyberspace capabilities.

Authoritarian governments are working to weaken global commitment to universal human rights enshrined in the Universal Declaration of Human Rights and international legal instruments, such as the UN Charter and the International Covenant on Civil and Political Rights. Authoritarian governments, most notably the PRC, are actively working to co-opt and redefine well-established terminology related to "democracy" and "human rights" in the context of international technology policy development, including through their input into the UN Pact for the Future process and its Global Digital Compact.

Threats to Internet and Digital Freedom

Authoritarian and illiberal states are seeking to restrict human rights online and offline through the misuse of the Internet and digital technologies. Governments are closing and siloing the Internet: suppressing dissent through Internet and telecommunications shutdowns, virtual blackouts, restricted networks, and blocked websites.

The PRC has developed a massive system of surveillance, and its firms are now exporting their regulatory approach and technical capabilities to facilitate other governments' monitoring and repression. Beijing has also used cyber means to target people beyond its borders, including journalists, dissidents, and individuals it views as threats to Chinese Communist Party narratives, policies, and actions. In the wake of its full-scale invasion of Ukraine in 2022, the Russian government blocked access to foreign websites and increased

censorship and surveillance of domestic users. The Iranian government continues to rely on Internet restrictions, filtering, and surveillance to repress opposition to the regime.

A growing number of governments, including backsliding democracies, are misusing digital tools in ways that violate or abuse the individual's right to be free from arbitrary or unlawful interference with one's privacy, and restricting and threatening individuals' rights to freedoms of expression, association and peaceful assembly. Commercial spyware, AI-enabled facial recognition software, and other surveillance technologies are misused against journalists, human rights defenders and other activists, women, and members of marginalized groups, including beyond countries' borders. Technology-facilitated gender-based violence (TFGBV) chills speech, impedes privacy and freedom of expression, and undermines the ability of women, girls, and LGBTQI+ individuals to participate in democracy, governance, and civic life.

The proliferation of online manipulation, in combination with threats posed by foreign adversaries seeking to interfere with information integrity, pose fundamental threats to democracy, undermining trust in institutions, threatening electoral processes, and sowing discord within and between countries. PRC actors have increased their capabilities to conduct covert influence operations and disseminate disinformation. Even if Beijing sets limits on these activities, individuals not under its direct supervision may attempt election influence activities they perceive are in line with the PRC's goals. The Russian government remains a serious foreign influence threat because of its wide-ranging efforts to try to divide Western alliances and undermine U.S. global standing. Recently, Russian influence actors have adapted their efforts to better hide their hand.

Challenges of the Digital Economy

Some 2.6 billion people still do not have access to the Internet, leaving a third of the world unconnected. This situation presents an economic development challenge for many countries and a strategic challenge for the United States and its allies and partners. Left unaddressed, the digital divide not only imperils efforts to build a strong digital ecosystem, but also threatens to increase income inequality and instability in emerging economies. The digital divide disproportionately affects women and other marginalized groups. For example, 80 percent of women in low-income countries do not use the Internet. **[4]**

As the world has increasingly digitalized, countries around the world are grappling with how to approach the digital economy in a way that takes advantages of its benefits, addresses its

risks, and expands its reach to more people. Governments are developing differing regulatory approaches to a range of policy issues, such as protecting children's safety, health, and privacy, tackling TFGBV, addressing anti-competitive behavior, guaranteeing equitable access to connectivity and technology, building trusted digital infrastructure, and promoting trusted cross-border data flows.

A growing number of countries are promoting digital public infrastructure (DPI) as critical to achieving economic growth, good governance, and the UN sustainable development goals (SDGs). The definition of DPI is evolving, but generally encompasses networked open technology standards designed for the public interest, an enabling regulatory environment, and a community of market players driving innovation. While some of the most prominent models have included digital identification, digital payments, and data platforms for sharing and storing data, there is no one-size-fits-all solution. DPI models need to be grounded in safeguards, including human rights protections, and such models should be interoperable.

U.S. government and private sector actors seek to leverage data and the digital economy for positive economic and social benefits: preserving openness while protecting privacy, promoting safety, and mitigating harms. The Department of State, working with other agencies, looks to shape markets and safeguard innovation from regulatory excesses. Although there is an increasing willingness by some countries to embrace narratives of digital sovereignty and protectionism by blocking access to their markets, unduly preventing cross-border data flows, and preferencing domestic manufacturers and service providers, we continue international engagement to enhance interoperability, security, and market access.

Many states are promoting digital technologies for economic growth while trying to maintain autonomy and neutrality. They are looking to build digital infrastructure quickly and cheaply and seeking assistance to combat cybercrime and develop cybersecurity capacities. Yet the PRC government distorts markets to advantage PRC-based hardware, software, and services suppliers that compromise the security of the customer. By contrast, the United States seeks to provide the emerging and developing world with financially sound alternatives to unsustainable initiatives. The Department of State is committed to working with allies and partners to offer and deploy secure technologies that allow countries and civic actors around the world to build digital infrastructure and improve cybersecurity across sectors, offering direct benefits to governments while helping to ensure the protection of the human rights and privacy of their citizens that will enable an inclusive digital economy.

The Future of AI Technologies Governance

The uncertainty and complexity that characterizes the geopolitical competition over these digital technologies is compounded by the fact that we sit at the cusp of another technological revolution. The revolution in AI systems may occur at an even faster pace than the development and adoption of the Internet. AI technologies could be powerful tools for expanding knowledge, increasing prosperity and productivity, and addressing global challenges, and AI tools may help advance the seventeen UN SDGs. AI applications have the further potential to improve many aspects of citizens' lives including food security, health applications, good governance and democratic consolidation, and natural disaster preparedness and prevention.

The rapid growth of AI technology, however, comes with the significant risk that its use may exacerbate inequality and economic instability, stifle competition, cause consumer harm, aggravate discrimination and bias, invade privacy, enhance malicious cyber activity, and improve authoritarian capabilities for surveillance and repression. AI will challenge how we compensate for the uses of intellectual property as well as authenticate, label, or detect synthetic content. AI may also require workforce adaptations across economies; the rising energy demands of high-end AI chips and data centers could become a significant barrier to developing local capabilities.

Further, state and non-state actors have been observed using generative AI systems for malicious purposes, including to manipulate and disseminate disinformation at speed and scale. Many AI technologies are also dual use, lending themselves to new military and national security capabilities that may lack appropriate human rights and civil liberty protections and other safeguards. AI can advantage both the attacker and defender in cyberspace, and the systems themselves are subject to data poisoning and other types of malicious activities.

The question of how to balance risk and rewards looms large for governments and civil society around the world. The United States is working with allies and partners to move quickly to address the ways in which artificial intelligence can potentially destabilize societies while preserving its benefits—and, crucially, staying true to democratic values and protecting human rights. A critical part of this work is not only safeguarding an open and independent research environment but also partnering with emerging economies in the development and deployment of AI technologies. Helping to provide unrestricted access to an open,

interoperable, reliable, and secure Internet while demonstrating how AI can serve a shared agenda across the globe can help reduce the risk that the AI revolution will contribute to global instability and diminish our ability to address global challenges.

Working with the Private Sector and Civil Society

Competition, consumer choice, vibrant private sector investment, and a robust civil society are the hallmarks of an open, inclusive, and secure digital ecosystem. The Department of State cannot accomplish its objectives without strong partnerships with the private sector, civil society, academic, and technical communities. New innovations spring from the private sector, and the decisions tech companies make on how their systems are developed and deployed have profound implications for how U.S. values and interests are realized—including protecting users' safety and privacy. U.S. officials rely on a range of private sector, academic, and civic actors for insights into technology developments, and private sector and trade association stakeholders often provide early warning of discriminatory regulations that explicitly target American companies. Trusted technology suppliers, including small- and medium-sized enterprises, are essential partners in efforts to expand connectivity through open, secure, and resilient networks across the globe.

Civil society groups are working to ensure that individuals can access and pursue opportunities online free from unlawful surveillance and privacy-invasive data collection practices and are working to counter harmful propaganda and disinformation in digital spaces. Civil society and the technical community are often the first to recognize, warn of, and seek solutions to threats to human rights online and offline. As Internet freedom continues to decline in parts of the world, civil society activists, human rights defenders, and the journalists covering their activism are often leading the push back in digitally repressive societies, often at great personal risk. Additionally, civil society, the academic and technical community, and private sector actors play a crucial role in upholding the multistakeholder model of Internet governance, which is increasingly under threat.

The private sector, civil society, and the technical community are essential in helping defend against malicious cyber activities. In 2022, the private sector aided Albania in the wake of Iranian cyberattacks and, during Russia's full-scale invasion of Ukraine, technology firms and cybersecurity companies provided services, tools, and threat intelligence to help Ukraine defend government and critical infrastructure networks. They migrated data storage and cloud hosting services to counteract Russian efforts to erase critical data and provided

Internet and telecommunication services that helped keep government agencies and businesses operating. Non-governmental organizations and academic research groups have exposed the threat posed by the proliferation and misuse of commercial spyware against journalists, activists, and marginalized groups.

Public-private partnerships are essential to cyber and digital diplomacy, and they need to be flexible and adaptable. Cyber defense may require new ways to scale, supply, and license cyber defense services and products in a crisis and may be difficult to launch and sustain in a different regional context. Repressive governments are developing new methods to control digital technologies and to manipulate and interfere with information flows. To address these and other evolving challenges, the Department of State will continue to expand contact with and solicit input from a wide range of civil society and private sector actors. In addition, the United States will continue to work with allies and partners to advance a multistakeholder approach to digital and data governance.

Building Digital Solidarity

The United States believes digital technologies can and should be used to put people on a path to prosperity, solve global challenges, and build a better future for all. The Department of State will work with allies, partners, and stakeholders to promote an affirmative vision for cyber and digital technologies: one in which people around the world use cyberspace and digital technologies to advance economic prosperity and inclusion; enhance security and combat cybercrime; promote and protect human rights, gender equity and equality, democracy, and the rule of the law; and address transnational challenges. As part of this approach, the United States, allies, and partners will demonstrate the advantages of an open, interoperable, secure, and reliable Internet; serve as the partner of choice in the research, design, development, and deployment of digital and emerging technologies; and jointly impose consequences for behavior that runs counter to internationally accepted norms of state behavior. The Department of State will also work with and support emerging economies' efforts to improve cybersecurity and increase their cyber-resilience.

Each of the Strategy's four action areas—promote, build, and maintain an open, inclusive, secure, and resilient digital ecosystem; align rights-respecting approaches to digital governance; advance responsible state behavior, counter malicious activity, and offer mutual support; and strengthen digital and cyber capacity building assistance—reflects aspects of the Department of State's vision of digital solidarity. Moving forward, the Department of State will work to bring a wide range of partners across the globe into the process of building and

extending digital solidarity. We welcome all those who seek to develop and deploy technologies that are open and secure, promote inclusive growth, foster resilient and democratic societies, and empower all, including the most vulnerable.

Figure 2. Secretary Blinken and Deputy Secretary Sherman Visit the new Cyberspace and Digital Policy Bureau at the U.S. Department of State in Washington, D.C., on April 4, 2022. (U.S. Department of State photo.)

ACTION AREA 1: Promote, Build, and Maintain an Open, Inclusive, Secure, and Resilient Digital Ecosystem

Digital solidarity rests on and is reinforced by innovation across an open, inclusive, secure, and resilient digital ecosystem. Though the United States is a major power in digital, critical, and emerging technologies, we are not able to—nor should we—go it alone. Rather, the United States, allies, and partners are all made more prosperous, self-determining, and resilient when we work together to catalyze, support, and sustain rapid technological development on a range of critical technologies.

In close coordination with allies, partners, the private sector, and civil society, the Department of State continues to campaign for open, interoperable, secure, trusted, and reliable telecommunication networks, especially on fifth-generation wireless networks (5G). The White

House, Department of State, USAID, Department of Commerce, and the Federal Communications Commission (FCC) are engaged in discussions with allies and partners about deploying 5G mobile networks using trusted vendors and the future of 6G. Digital technologies are not limited to wireless technologies, and the Department of State and other agencies are coordinating with allies and partners on the development, deployment, and security of cloud infrastructure and data centers, undersea cables, and satellite communications. In addition, at all UN bodies the United States aims to promote—at a high level—the development, deployment, and use of rights-respecting digital technologies.

Line of Effort 1: Promote Development and Adoption of Open, Inclusive, Secure, and Resilient Telecommunication Networks

5G applications are rapidly evolving—expanding digital connectivity in new ways and creating new cybersecurity vulnerabilities. Telecommunication networks should be built using products from trusted suppliers that operate, and have supply chain partners that operate, primarily in countries that respect rights through consistent application of the law through an independent judiciary, in accordance with the principles reflected in the Organisation for Economic Co-operation and Development (OECD) Declaration on Government Access to Personal Data Held by Private Sector Entities. Telecommunications networks should not be built using products from suppliers subject to the control or influence of an authoritarian regime, and without meaningful, independent checks and balances or judicial recourse against government demands. International 5G-related principles, such as the Prague Proposals on 5G Security and Prague Proposals on Telecommunications Supplier Diversity, support market competitiveness and the diversity of trusted 5G equipment vendors.

These efforts also extend to the Partnership for Global Infrastructure and Investment's Digital Infrastructure pillar. Recognizing that cost is often the primary driving factor in ICT procurements, the United States is supporting governments, middle-mile internet infrastructure providers, and Internet service providers to develop greater competition and diversity in telecommunications supply chains, particularly through the Digital Connectivity and Cybersecurity Partnership (DCCP). DCCP is a whole-of-government effort, led by the Department of State, to provide capacity building, technical assistance, and project design and financing in support of an open Internet and enhanced cybersecurity.

In addition, the CHIPS and Science Act allocated $500 million to the International Technology Security and Innovation (ITSI) Fund for the Department of State to support the development and adoption of secure semiconductor supply chains and telecommunications networks. The

United States will use this funding to continue to work with partners to put in place policy and regulatory frameworks for secure ICT ecosystems and to level the playing field for secure and trustworthy vendors.

Along with helping build secure networks, digital solidarity is also expressed through efforts to build digital infrastructure that promotes competition, advances consumer choice, and puts communities and individuals in charge of their digital lives and resources. Recognizing the need to attract capital and de-risk potential digital infrastructure investment, USAID—with funding from DCCP—launched a blended finance program called Digital Invest that partners with fund managers and project developers to expand access to Internet connectivity and digital financial services in emerging markets worldwide. To date, Digital Invest's 13 partners have leveraged an initial $8.45 million in Department of State and USAID funding to raise over $300 million in investment capital for digital finance and Internet service providers in emerging markets that use secure network equipment, catalyzing an additional $1.15 billion in follow-on funding from third-party investors.

U.S. foreign assistance programs will also increase competition in the market and promote telecommunications supplier diversity by advancing the development of open and interoperable interfaces and protocols, such as Open Radio Access Networks (Open RAN). This open network architecture eases the ability for new suppliers to enter the market, lowers costs for deployment, and speeds innovation. Open RAN presents opportunities for emerging economies to participate directly in the supply chain, such as through local assembly and software development. Just as important, Open RAN offers alternatives for the reliance on technology from untrusted vendors. As a result, the Department of State will continue to support efforts such as funding commercial trials, feasibility studies, reverse trade missions, and workforce education and awareness activities that promote Open RAN. The United States will continue collaborating with the governments of Australia, Canada, Japan, and the United Kingdom on telecommunications supply chain diversification and related issues through the Global Coalition on Telecommunications, launched in October 2023.

Working with other governments and the private sector, the United States is also preparing for a new wave of innovation. Within the next decade, 6G will within the next decade bring even higher speeds, larger capacity, and lower latency to wireless communication. Building open and interoperable network architectures such as Open RAN into 6G development from the beginning will help ensure supplier diversity and supply chain resilience. In February 2024, the United States—with Australia, Canada, the Czech Republic, Finland, France, Japan, the Republic of Korea, Sweden, and the United Kingdom—endorsed shared principles for the research and development of 6G wireless communication systems.

Line of Effort 2: Further Common Understandings and Shared Principles for the Secure Use and Trustworthiness of Cloud Services, Data Centers, and Related Infrastructure Technologies

Cloud computing has become an essential enabler of the digital transformation of economies and businesses. By providing on-demand access to scalable computing resources in a reliable and cost-effective manner, cloud services allow governments and businesses to deliver more secure and resilient services to their citizens and customers. Moreover, cloud services were proven to be a strategic asset as Russian forces physically destroyed Ukrainian facilities holding critical data. Migration of government information technology infrastructure to the cloud improved resilience and preserved information essential to the operation of the economy and government.

U.S. cloud computing and data center firms compete globally and offer services to a broad international customer base while, in parallel, the United States government actively partners with foreign governments to promote the fair and safe use of cloud computing resources. At the same time, providers from authoritarian states are globalizing, and they are often more responsive to short-term local economic development goals, providing packages that include financial subsidies, local cloud infrastructure, and workforce training. Cloud services and data centers are also a source of tension with close trade partners. Some have threatened to exclude U.S. cloud providers from their markets in part because of concerns about access to and control of data, despite the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act providing for agreements to allow for consistent protections based on the rule of law. The Department of State is committed to reaching a common understanding with our international partners on the fair and safe use of cloud computing resources.

In addition, the Department of State will work with international partners and the private sector to address the costs and increase support for building secure cloud infrastructure in emerging economies. DCCP is reinforcing these efforts through the support of feasibility studies, reverse trade missions, financing, and training programs, such as training grants in the Philippines to support the provision of cloud computing capabilities.

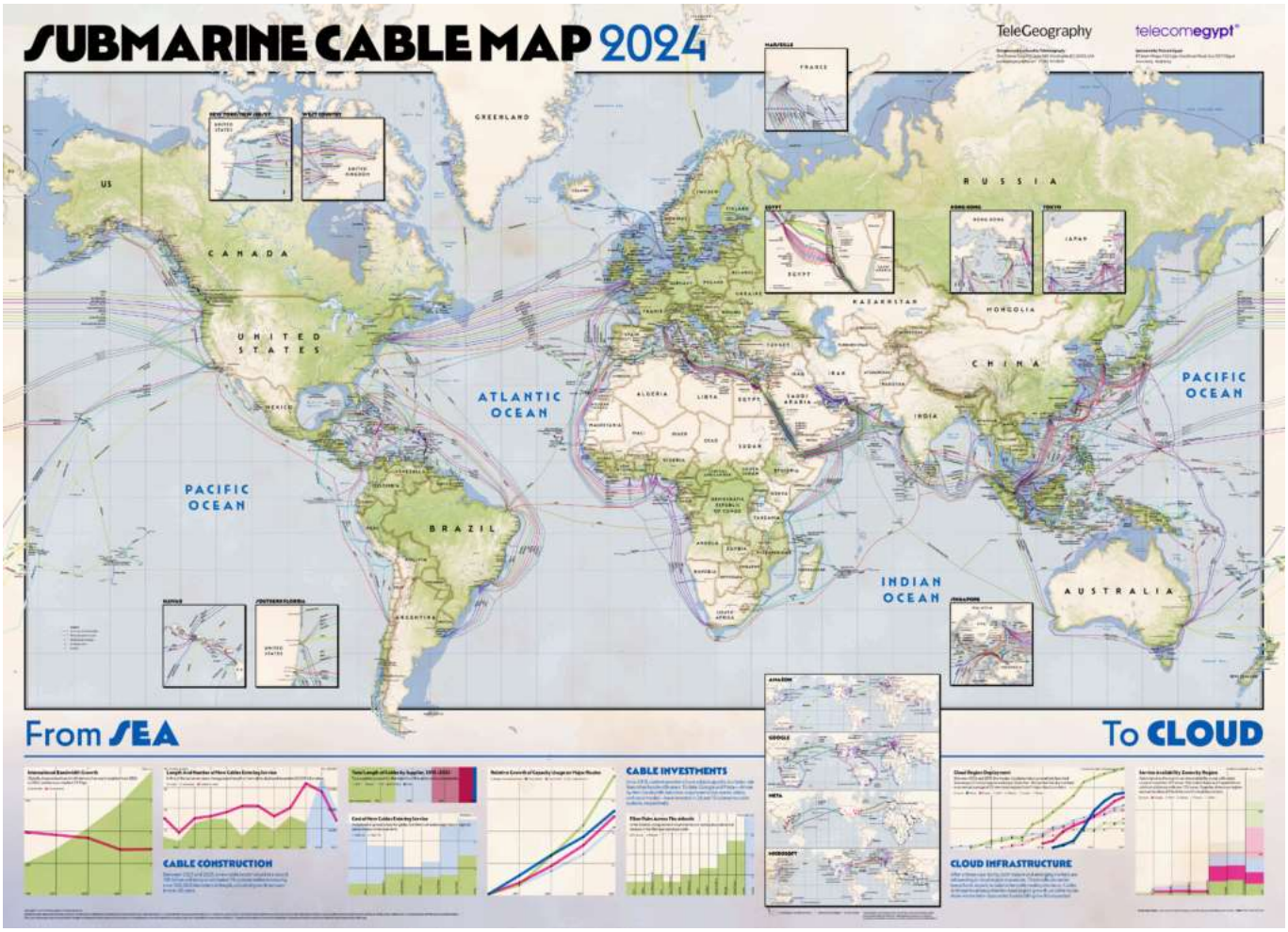

Figure 3. Global Submarine Cable Map 2024. (Illustration by TeleGeography)

Line of Effort 3: Enhance Security and Resilience of Undersea Cables

Undersea cables carry more than 95 percent of the world's digital traffic. As data continues to proliferate and increase exponentially, so too does demand for cables and other transmission systems. Disruption or destruction of the cables as a result of accidents, natural disasters, or malicious actions could isolate a county, threaten national security, and result in billions of dollars of damage to the economy. Choices made about which vendors to rely on for undersea cable infrastructure, maintenance, and repair operations can either drive development and innovation or lead to new forms of dependency and insecurity. As a result, the Department of State, in coordination with other agencies, will prioritize enhancing the security and resilience of undersea cables.

U.S. firms and other trusted suppliers are leading producers of many network components, embedded technologies, and related services for undersea cables, and they are investing in and financing new undersea cables connecting all regions of the world. The U.S. government will continue to support U.S. and other trusted suppliers in the installation, operation,

maintenance, and repair of secure infrastructure as well as to promote a regulatory environment that enables continued investments.

Since 2021, the Department of State has implemented the CABLES program throughout the East Asia Pacific region, responsibly informing essential telecommunications and cables infrastructure stakeholders of the perils of choosing untrusted suppliers. The United States provided capacity building to support five countries using U.S. technology for the South-East Asia-Middle East-Western Europe 6 cable (SMW6), and separately it provided over $22 million in partnership with Australia and Japan to help fund the East Micronesia Cable being built by a Japanese firm. In October 2023, the United States announced that, working with Congress, it would provide, along with Australia, investments totaling $65 million to fund future undersea cable connectivity for Pacific Island countries in order to facilitate access to global markets and the realization of regional connectivity goals. In support of these policy objectives, the United States will continue engaging with the G7 and other multilateral groups to strengthen trusted, multi-layered global connectivity that provides data route diversity, resiliency, and redundancies.

Line of Effort 4: Pursue Shared Interests in the Development, Use, Resilience, and Security of Satellite Communication Networks

Satellite communications remain a vital capability for connecting the world and delivering global access to information. Geostationary orbit (GEO) satellites have served this mission for decades and will continue to do so for decades to come. Newly deployed satellite technologies, including low-earth orbit (LEO) satellites, are increasingly important to the United States, its allies, and partners as we work to connect the unconnected. The distributed nature of proliferated satellite constellations offers resilience, and LEO satellite communication services can increasingly be deployed rapidly to cover disaster or conflict zones. Moreover, the ability of LEO satellite services to bring broadband communications to almost every inch of the planet raises the possibility of expanding Internet access in a rights-respecting manner, closing the digital divide, and advancing UN Sustainable Development Goals.

U.S. firms lead in the development and deployment of GEO and LEO satellite communication services, but other countries, including our strategic competitors, are investing in new technology capacities. The PRC is planning a constellation of about 13,000 satellites, with a clear government mandate and significant financial subsidies. Some states, concerned that

LEO satellite capabilities will undermine their ability to control information flows, are raising market access barriers, such as setting stringent domestic equipment requirements or forbidding foreign ownership. Some governments and non-government stakeholders have also raised concerns in multilateral bodies about increased space debris, interference with astronomy, increased cases of radio frequency interference among LEO satellites or from LEO to GEO satellites, and other potential negative impacts of LEO satellite networks. Some countries, although they are interested in the connectivity benefits LEO satellite systems could bring, are unfamiliar with the systems and lack effective regimes to support market entry and licensing. In addition, space systems and assets introduce vulnerabilities to U.S. and allies' critical infrastructure that our adversaries are willing to exploit.

The Department of State will cooperate with partners and allies to pursue shared interests in the development, use, resilience, and security of LEO satellite systems. The Department of State will work to expand global access to secure services through the International Telecommunication Union (ITU), remove barriers to LEO satellite system providers, and increase multilateral assistance for satellite services for underserved areas. The Department of State, along with other agencies, will also facilitate international cooperation on research and development in LEO satellites. The United States will also promote norms, guidelines, and best practices, including the development of licensing and regulatory regimes, for the secure, safe, and sustainable use of LEO satellites, as well as work with allies and partners on enhancing space cybersecurity and critical infrastructure resilience and security.

Line of Effort 5: Enhance the International Telecommunication Union's Effectiveness, Transparency, and Accountability

Responsible, forward-looking, inclusive, and transparent leadership by the ITU on telecommunications standards, telecommunications and ICT development, closing digital divides, and radio frequency spectrum is vital to U.S. development, defense, and economic priorities. The United States has long supported the work of the ITU in its core competencies, including global radiofrequency spectrum harmonization and advancing the development of the world's telecommunications networks by enhancing connectivity and interoperability. Since Secretary-General Doreen Bogdan-Martin's 2022 election, the United States has been working with other member states and partners to help her deliver on her vision to expand digital connectivity and inclusion; strengthen partnerships and stakeholder collaboration; empower and engage youth; and enhance the ITU's organizational effectiveness, transparency, and accountability to achieve its overall goals.

ACTION AREA 2: Align Rights-Respecting Approaches to Digital and Data Governance with International Partners

Digital solidarity recognizes the necessity of the domestic governance of digital and emerging technologies but seeks to develop shared mechanisms that will help maintain an open, interoperable, secure, and reliable Internet as well as trusted cross-border data flows. It works to foster democratic values-based and rights-respecting policies.

To advance the NSS and the NCS effectively, promoting, building, and maintaining a secure digital ecosystem must be accompanied by efforts to make digital and data governance compatible across allies and partners through greater alignment, mutual recognition, and reciprocity of policies. The Department of State, along with other federal agencies, is building and reinforcing digital solidarity through support for the trusted flow of data; advocacy for multistakeholder, risk-based approaches to digital and data governance; and the promotion of shared values and governance principles for critical and emerging technologies. The Department of State, in collaboration with the Department of Commerce and other agencies, is expanding its capacity to engage in international standards development organizations and to coordinate with industry and civil society to ensure robust participation by U.S. stakeholders in standards setting processes and other international fora. The United States is also working with allies and partners to advance a common, rights-respecting vision for the digital future; negotiate a rights-respecting cybercrime treaty; and defend information integrity.

Line of Effort 1: Support the Trusted Flow of Data and Advocate for Multistakeholder, Risk-Based Approaches to Digital and Data Governance

Digital solidarity is further built and reinforced through the joint development, harmonization, and mutual recognition of rights-respecting approaches to data governance and digital trade. This work is currently ongoing through mechanisms such as Indo-Pacific Economic Framework for Prosperity (IPEF), Digital Transformation with Africa initiative (DTA), the Americas Partnership for Economic Prosperity (APEP), the G7, OECD, TTC, and the Quad.

The United States supports the trusted free flow of data and an open Internet with strong and effective protections for individuals' human rights and privacy and measures to preserve

governments' abilities to enforce laws and advance policies in the public interest. Legitimate concerns about data privacy can be addressed through protective mechanisms that follow the data while at the same time facilitate cross-border data flows and strengthen global cooperation among enforcement authorities. The United States will continue championing trusted cross-border data flows by promoting data transfer mechanisms that improve interoperability between different data privacy regimes. Working alongside our interagency partners, the Department of State supported the negotiation and implementation of the EU-U.S. Data Privacy Framework; the development of the OECD Declaration on Trusted Government Access to Data Held by the Private Sector, which identifies commonalities in the privacy safeguards democratic governments follow when accessing data for legitimate law enforcement and national security purposes; as well as initiatives on Data Free Flow with Trust at both the G7 and the OECD. The Department of State works with the Department of Justice to clarify application of the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act and to negotiate bilateral agreements under the act.

Along with Australia, Canada, Japan, the Republic of Korea, Mexico, the Philippines, Singapore, and Taiwan, the United States launched the Global Cross-Border Privacy Rules (CBPR) Forum in April 2022, building on the previously established Asia Pacific Economic Cooperation (APEC) CBPR system. The CBPR provides a data privacy certification backed by relevant authorities that facilitates data flows by promoting interoperable, enforceable data protection standards. Officials from the Departments of State and Commerce will continue efforts to bring new countries into the agreement, building on efforts such as workshops held in Kenya, Mexico, Chile, Brazil, UK, Israel, Jordan, Panama, Colombia, Fiji, and Barbados as well as ASEAN countries.

While the United States and its likeminded trade partners share many of the same values, we often have differing approaches to how to regulate the digital economy. The U.S. government advocates for multistakeholder, risk-based approaches that target the challenges we face while providing the flexibility to realize the benefits of new and emerging technologies. Unilateral approaches in digital taxation and the imposition of network usage fees often do not address the core issues of accessibility and fairness expressed by their proponents. Additionally, the rise of a growing digital sovereignty narrative that has been embraced by some of our close partners and allies has the potential to undermine key digital economy and cybersecurity objectives. The Department of State, working with other agencies, will continue to argue against data localization, network usage fees, digital services taxes as well as other market access barriers that contribute to the perception of increased control, but in reality often can undermine growth and security objectives.

Line of Effort 2: Promote Common Understandings of Trust, Interoperable Standards, and Shared Values and Governance Principles for Critical and Emerging Technologies

One of the most pressing challenges for digital solidarity is developing common approaches to governing critical and emerging technologies such as AI. The speed of innovation, the scale of the competition, and the stakes for our values, security, and prosperity demand concerted action. With AI technologies, we will not have the luxury of time or of pursuing narrow interests that have often slowed our ability to develop shared principles and interoperable regulatory approaches in other parts of the digital economy.

Shaping shared values and governance principles on the development, deployment, and use of AI is increasingly central to American digital diplomacy. The United States is engaging allies, partners, the private sector, civil society, the technical community, and other stakeholders in discussions at the G7, Global Partnership on Artificial Intelligence, the Council of Europe, OECD, UN, UNESCO, and other fora to manage the risks of AI and ensure its benefits are widely distributed. In addition, we will need to work together to invest in the science research and infrastructure necessary to measure, evaluate, and verify advanced AI technology systems.

In July 2023, President Biden announced voluntary commitments from seven leading AI companies to advance the safe, secure, and transparent development of AI technology. Eight more companies (including one foreign-based company) signed on to the commitments in September. The United States internationalized and expanded on the voluntary commitments through the G7 Hiroshima AI process led by Japan to tackle generative AI, with leaders releasing an International Code of Conduct for Organizations Developing Advanced AI systems in October 2023. We continue to work on broadening acceptance of the Code of Conduct by more countries and companies beyond G7 member countries.

The United States joined twenty-seven other countries at the UK AI Safety Summit and signed the Bletchley Declaration, which encourages transparency and accountability from actors developing frontier AI technology. The United States and the United Kingdom have also signed a memorandum of understanding between their respective AI Safety Institutes advancing the science of measuring, evaluating, and addressing AI risks as a first step toward a global consensus on the scientific underpinnings of AI safety. These efforts outline a role for national governments, promote international cooperation, and encourage innovation by

providing technically rigorous guidelines for introducing safe, secure, and trustworthy AI technology. At the same time, USAID and several other international development donors entered into a partnership to promote safe, secure, and trustworthy AI development in low- and middle-income countries in Africa and other parts of the world.

Hiroshima Principles for Generative AI

Take appropriate measures throughout the development of advanced AI systems, including prior to and throughout their deployment and placement on the market, to identify, evaluate, and mitigate risks across the AI lifecycle.	**Develop and deploy reliable content authentication and provenance mechanisms, where technically feasible, such as watermarking or other techniques to enable users to identify AI-generated content.**
Identify and mitigate vulnerabilities, and, where appropriate, incidents and patterns of misuse, after deployment including placement on the market.	**Prioritize research to mitigate societal, safety and security risks and prioritize investment in effective mitigation measures.**
Publicly report advanced AI systems' capabilities, limitations and domains of appropriate and inappropriate use, to support ensuring sufficient transparency, thereby contributing to increase accountability.	**Prioritize the development of advanced AI systems to address the world's greatest challenges, notably but not limited to the climate crisis, global health and education.**
Work towards responsible information sharing and reporting of incidents among organizations developing advanced AI systems including with industry, governments, civil society, and academia.	**Advance the development of and, where appropriate, adoption of international technical standards.**
Develop, implement, and disclose AI governance and risk management policies, grounded in a risk-based approach – including privacy policies, and mitigation measures, in	**Implement appropriate data input measures and protections for personal data and intellectual property.**

particular for organizations developing advanced AI systems.

Invest in and implement robust security controls, including physical security, cybersecurity and insider threat safeguards across the AI lifecycle.

In October 2023, President Biden issued an Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. This Order establishes a process to develop new standards for AI safety and security and seeks to protect citizens' privacy, promote innovation and competition, and advance equity and human rights. The Order tasked the Department of State with strengthening U.S. leadership abroad on AI issues. The Department of State and USAID, in collaboration with the Department of Commerce, are leading an effort to establish an AI in Global Development Playbook to harness AI's benefits and manage its risks. Relatedly, the Department of State plans to lead an interagency task force on detecting, authenticating, and labeling synthetic content, which aims to facilitate information sharing and mobilize global commitments to both label authentic government-produced content and detect synthetic content. In addition, working with the Department of Homeland Security (DHS), the Department of State is engaging international partners to help prevent, respond to, and recover from potential critical infrastructure disruptions resulting from the incorporation of AI into critical infrastructure systems or the malicious use of AI against those systems. The Department of State and USAID are also working with interagency partners, including the National Institute of Standards and Technology (NIST), National Science Foundation (NSF), and Department of Energy, to develop a human rights risk management framework for AI and a global AI research agenda.

The Department of State is also building broad-based support for the Political Declaration on Responsible Military Use of AI and Autonomy. While there are important discussions ongoing in Geneva under the framework of the Convention on Certain Conventional Weapons (CCW) – which the United States will continue to support – the scope of those discussions only covers one possible military use of AI, namely autonomous weapon systems. The Political Declaration is the first effort to articulate principles and best practices covering all military applications of AI technologies.

Line of Effort 3: Ensure International Standards Processes are Transparent, Open, Inclusive, and Impartial

International technology standards facilitate technology advancement, trade, global economic growth, and market access, particularly for startups and small- and medium-sized enterprises. They are also an area of strategic and economic competition, with the PRC in particular pushing top-down approaches to standards development process and using its economic influence to compel support for its standard proposals. In May 2023, the Biden-Harris White House published the first ever U.S. Government National Standards Strategy for Critical and Emerging Technology (USG NSSCET). As outlined in the USG NSSCET, the United States will work with allies, partners, the private sector, and civil society to ensure that international standards development embraces transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and broad multistakeholder participation. The Department of State, in cooperation with the Department of Commerce and other agencies, is building enhanced capacity to engage directly in international standards development organizations and to coordinate with industry and civil society to ensure robust participation by U.S. stakeholders in standards making processes.

Working with the FCC, NIST, National Telecommunications and Information Administration (NTIA), and other federal agencies, the Department of State supports standards development processes for a wide range of critical and emerging technologies and platforms, including IoT, energy grids, smart cities, and connected vehicles. The United States will continue to promote and leverage cybersecurity and privacy standards and guidelines developed by NIST through open processes with a strong connection to international standards.

This approach reinforces the U.S. policy for standards: a private-sector led, industry-driven approach with government participation that emphasizes the use of international standards developed in open, transparent, and consensus-based processes. This alignment helps stakeholders reduce the burden of international regulatory and legal regimes, leading to a reduced cost of operation and a greater understanding of international policies. It also highlights the value of a bottom-up approach for other governments as they develop their cybersecurity priorities.

The U.S. government has developed formal and informal methods of information sharing and standards development monitoring through regular engagement with partners and allies. Quad partners and members of the TTC, for example, have signed memoranda of

cooperation to enable increased information sharing, coordination, and influence in international standards development. The Department of State has also supported increasing participation in standards development organizations from historically underrepresented nations.

Line of Effort 4: Expand and Diversify Civil Society Participation in Multistakeholder Processes

The United States and its partners remain committed to the multistakeholder model of Internet and digital governance. Active and meaningful participation of all stakeholders, including governments, civil society, the private sector, academia, and the technical community, is essential to informing our discussions and policymaking, promoting transparency and accountability, and strengthening implementation and sustainable development. Through foreign assistance programs, the Department of State is advancing policy and advocacy initiatives through which civil society stakeholders engage with national governments, regional governance bodies, and international standard-setting entities to encourage Internet and digital governance policies consistent with democratic values and international human rights. The Department of State will continue its efforts to expand and diversify the groups who are working to promote interoperable, rights-respecting, and secure digital technologies. It will also continue to prevent and defend against efforts by repressive governments to exclude civil society and other stakeholders from participation in relevant fora.

The United States strongly supports the Internet Governance Forum (IGF) as the preeminent global body bringing together all stakeholders through a bottom-up process to discuss rights-respecting solutions to Internet public policy issues. It will continue to work with allies and partners to sustain and bolster the IGF's relevance.

Line of Effort 5: Advance a Common, Rights-Respecting Vision for the Digital Future

Digital solidarity is built on a shared commitment to human-rights based technology governance. The Advancing Digital Democracy (ADD) initiative, launched by USAID at the Summit for Democracy in 2021, fosters an open, secure, and inclusive digital ecosystem through programs such as partnerships with governments, private sector and civil society to

strengthen legal and regulatory frameworks for data and digital technologies, and increased support for software engineers, tech companies, and researchers working to embed respect for human rights and democratic values across the tech lifecycle. In April 2022, the United States and 60 countries launched the Declaration for the Future of the Internet (DFI), bringing together a broad, diverse coalition of partners around a common, rights-respecting vision for an open, interoperable, reliable, and secure digital future. As chair of the Freedom Online Coalition in 2023, the United States prioritized protecting fundamental freedoms online; countering and building resilience to the misuse of digital technologies; advancing norms, principles, and safeguards regarding the development and use of artificial intelligence; and strengthening digital inclusion. Similarly, the United States, working with 13 other countries, launched the Global Partnership for Action on Gender-Based Online Harassment and Abuse. This partnership, which emerged from the first Summit for Democracy, is a response to the need to address technology-facilitated gender-based violence as part of a shared global agenda to promote peace, security, and stability.

The United States will continue working with allies and partners to ensure digital technologies are used in a responsible and rights-respecting manner. Along with 45 partners, the United States endorsed in March 2023 Guiding Principles on Government Use of Surveillance Technologies, which are intended to prevent the misuse of surveillance technologies by governments. In addition, the Department of State will continue to advance programs that enable at-risk, vulnerable, and marginalized populations, or those who protect them, to prepare for, prevent, identify, investigate, and obtain remedy for digital abuses or other types of digital repression.

The United States supports several multistakeholder efforts working to address a range of online challenges while respecting freedoms of opinion and expression, including the Christchurch Call to Action in 2019, the French-led Child Online Protection Laboratory, Freedom Online Coalition, and the Global Partnership for Action on Gender-Based Online Harassment and Abuse. The United States will continue to advocate for a rights-respecting approach consistent with protecting freedoms of opinion and expression and promoting gender equity and equality as governments around the world propose increased regulation of online platforms.

Further strengthening domestic policy will enable deeper coordination with international partners on a range of digital issues. The Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, for example, has reinforced the position of the United States in international discussions on the governance of AI. The National Cybersecurity Strategy supports legislative efforts to impose robust, clear limits on

the ability to collect, use, transfer, and maintain personal data and provide strong protections for sensitive data like geolocation and health information. The NCS specifically calls for this legislation to mitigate privacy risks arising from data processing and set national requirements to secure personal data.

Line of Effort 6: Negotiate a Rights-Respecting Cybercrime Treaty

The United States, its allies, and partners as well as civil society groups have long supported the Council of Europe Convention on Cybercrime (commonly known as the Budapest Convention) as the most effective tool for providing global standards for criminalizing malicious cyber activities, obtaining electronic evidence, and fostering international cooperation on computer-related crimes. The Convention was drafted to be global and open to all regions. Seventy-two countries, including the United States, are currently parties to the Convention, and 21 additional countries have been invited to accede.

While supporting accession to the Budapest Convention, the United States and its partners are also actively working to ensure that negotiations in the UN Ad Hoc Committee to elaborate a convention against cybercrime reach a positive outcome: a rights-respecting cybercrime treaty that would enable all UN member states to cooperate better in the fight against cybercrime. The United States and its partners will continue to oppose overly broad definitions of cybercrime that could be used to stifle freedom of expression, infringe on privacy, and or endanger individuals and communities. The United States will also continue to advocate for necessary and sufficient safeguards commensurate to the scope of the domestic powers and international cooperation provided for in the convention. Maintaining an open, inclusive, and transparent process will best allow states to negotiate a binding agreement with the participation of interested stakeholders.

Line of Effort 7: Defend Information Integrity

Information integrity challenges are not new, but determined foreign state adversaries and rapid technological advances, especially AI-enabled human-machine interactions, create complex dynamics that compound information risks by enabling rapid, large-scale, and targeted dissemination of AI-enabled synthetic content. Building a resilient information environment—one in which there is open, free public debate and consistent access to diverse sources of fact-based information—is an ongoing priority for the United States and its allies

and partners. These features are essential for citizens to inform their opinions and exercise their human rights, including freedom of expression, freedom of peaceful assembly and association, and the right to vote. Information manipulation is destabilizing and can harm national security, democratic processes, economic welfare, the environment, crisis response, human rights, and public health. While foreign actors seeking to interfere with or manipulate the information environment pose significant risks, there are additional challenges open societies face around the quality of information online and deteriorating trust.

With allies and partners, the Department of State will continue to work to build civic information resilience, counter foreign state and non-state extremist propaganda online, and mitigate risks of AI to information integrity while protecting freedom of expression. The U.S. Government will work to protect the integrity of elections and other democratic processes across the globe. At the TTC, OECD, and G7, the United States develops shared approaches to building healthy and resilient information ecosystems. The United States and France are co-chairing the DIS/MIS Information Resource Hub, the OECD's leading information integrity initiative. At the Hub, the Department of State is focused on increasing cooperation around sharing of best practices and strengthening information resilience, both among OECD and non-OECD countries, and developing a framework to guide whole-of-society efforts in this area. Through the Promoting Information Integrity and Resilience Initiative (Pro-Info), USAID aims to bolster healthy information ecosystems and help address information manipulation through multi-stakeholder engagement, donor coordination, and capacity building efforts.

At the third Summit for Democracy in 2024, the United States launched a democratic roadmap for building civic resilience to global digital manipulation that highlights the importance of the digital information manipulation challenge as a threat to the functionality and vitality of society; recognizes that building information integrity can be consistent with freedom of opinion and expression; reinforces private sector digital platforms' ability to strengthen civic resilience; and prioritizes efforts to address generative AI (GAI)—particularly in the context of global 2024 elections. The United States has also endorsed the Global Declaration on Information Integrity Online, launched by Canada and the Netherlands. The Declaration, grounded in international human rights law, establishes high-level international commitments by participating states to protect and promote information integrity online.

In addition, the Department of State has announced a Framework to Counter Foreign State Information Manipulation. This Framework seeks to develop a common understanding of the threat and establish a common set of action areas from which the United States, with its allies and partners, can develop coordinated responses to foreign information manipulation and protect free and open societies.

ACTION AREA 3: Advance Responsible State Behavior in Cyberspace and Counter Threats to Cyberspace and Critical Infrastructure by Building Coalitions and Engaging Partners

At the UN and regional security bodies, the United States, along with its allies and partners, is working to advance responsible state behavior in cyberspace based on a UN General Assembly-endorsed framework, underpinned by the applicability of existing international law, adherence to globally accepted and voluntary norms of state behavior in peacetime, development and implementation of confidence-building measures to reduce the risk of conflict in cyberspace, and a commitment to building states' capacities to implement the elements of the framework.

Despite a global consensus on the framework for responsible behavior in cyberspace, the norms are not self-enforcing. Some states act in ways contrary to it. When a state engages in significant destructive, disruptive, or otherwise destabilizing malicious cyber activity contrary to the framework, responsible states must cooperate to hold that irresponsible state accountable.

Digital solidarity in this context is demonstrated by sustained mutual support and coordinated campaigns. The United States and its partners share cyber threat information to help build resilience to and disrupt malicious activities; show solidarity to victims by helping respond to significant incidents, thereby signaling to adversaries they cannot isolate a target country through malicious operations; and ensure accountability for destructive, disruptive, and otherwise destabilizing cyber activities in concert with likeminded countries. The United States and some allies also have affirmed the application to cyberspace of their respective mutual defense treaty obligations. In addition, the Department of State and other federal agencies are working with allies and partners to disrupt ransomware and other criminal networks and safeguard democratic processes and institutions. Looking forward, the United States will continue efforts like these to advance responsible behavior in cyberspace, and counter threats to cyberspace and our critical infrastructure by building coalitions and engaging partners.

Line of Effort 1: Pursue Action-Oriented Discussions Focused on Norm Implementation at the UN

Sustained engagement over almost two and a half decades and across four previous administrations has yielded a framework of responsible state behavior in cyberspace repeatedly supported by all members of the UN General Assembly, which affirms the applicability of international law to states' use of information and communication technologies, endorses adherence to voluntary norms of responsible state behavior in peacetime, and proposes practical confidence-building measures to help reduce the risk of conflict stemming from cyber incidents. The framework is the core of our vision for a cyberspace in which states behave appropriately, manage the risk of unwanted escalation, hold bad actors accountable for irresponsible activities, and work together to respond to and recover from significant cyber incidents. Implementation of these norms, however, is critical to their effectiveness.

We will pursue more action-oriented discussions at the UN focused on how member states and institutions can work together to implement the framework's essential elements and build all states' capacity to manage cyber-related threats. To accommodate this evolving conversation, the United States and its partners have proposed a more action-oriented forum, a Program of Action (POA), as a future permanent mechanism for dialogue on cyber issues related to international security at the UN. Designed to be flexible enough to address future threats, with member states setting its direction over time, the POA will also incorporate the views of civil society, the private sector, and other non-state stakeholders.

As part of advancing responsible state behavior in cyberspace, the United States and our partners will also continue to work together in regional security and other fora, such as the Organization for Security and Cooperation, Organization of American States, and the ASEAN Regional Forum, to develop and implement cyber confidence building measures.

UN Framework of Responsible State Behavior

Figure 4. Four components that make up the UN framework of responsible state behavior in cyberspace. (Australian Strategic Policy Institute/United Nations General Assembly illustration.)

Line of Effort 2: Disrupt and Build Resilience to Malicious State Activity

Given the interconnected nature of cyberspace, international cooperation is crucial to deny, disrupt, and counter adversary activities in and through cyberspace.

The Department of State leads efforts, including facilitating international outreach, to address the rising threat of disruptive or destructive cyberattacks on the critical infrastructure of the United States and its allies and partners. This includes sharing through diplomatic channels joint cybersecurity advisories with the Cybersecurity and Infrastructure Security Agency

(CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA), and allies and partners on threats; capacity building and information sharing with new and existing partners to mitigate cyber threats and ensure the resilience of their critical infrastructure; and using bilateral, multilateral, and other fora to clarify and communicate expectations about adherence to international law and the framework for responsible behavior in cyberspace. In addition, members of the Quad have developed joint principles for the cybersecurity of critical infrastructure and NATO members have committed to ensuring the resilience of critical infrastructure, enhanced protection of critical infrastructure through training and exercises, and shared intelligence on threats.

As part of its counter adversary cyber activity, the Department of State provides foreign policy guidance and uses diplomatic engagements to support the Department of Defense (DoD)'s efforts to campaign in and through cyberspace below the level of armed conflict to reinforce deterrence and frustrate adversaries. As laid out in the 2023 DoD Cyber Strategy, U.S. Cyber Command continues to defend forward to discover, expose, and protect against the sources of malicious cyber activities and to reinforce responsible state behavior by encouraging adherence to international law and internationally recognized cyberspace norms. The DoD Cyber Strategy also notes that cyber operations are most effective when used in concert with other instruments of national power, including diplomatic engagement and cyber capacity building.

The Department of State, in close coordination with interagency and international partners, will continue to organize and execute sustained diplomatic pressure campaigns to raise international and public awareness of significant cyber threats and to increase the costs and risks to malicious cyber actors. For example, the United States has worked with allies, partners, and the private sector to disrupt DPRK revenue-generation efforts through cybercrime, crypto theft, and IT workers. U.S. Cyber Command, NSA, DHS, DOJ, and the FBI have exposed North Korean malware, seized malicious cyber infrastructure, seized cryptocurrency and fiat currency, and shared actionable threat intelligence with the private sector. The Department of State coordinates action with the Republic of Korea through a bilateral DPRK Cyber Working Group, including information sharing and policy coordination. Also, the United States, Japan, and the Republic of Korea coordinate efforts to counter DPRK cyber threats through a trilateral working group announced during the Camp David Summit in August 2023. The Department of State has also briefed officials around the world on threats posed by DPRK IT workers and cyber actors and deployed foreign assistance funds to build capacity to detect and defend against DPRK cyber and crypto threats.

Line of Effort 3: Support Allies and Partners Amid Malicious Activity

A core element of digital solidarity is standing with partners when they are impacted by significant disruptive or destabilizing cyber incidents. The Department of State will continue to work with allies and partners – through our embassies on the ground and our cyber experts in Washington – to coordinate appropriate support during the investigation, mitigation, and recovery from such cyber incidents. This support can include, as appropriate, the provision of advice by embassy cyber experts; facilitation of remote or on-the-ground investigative, hunt, and malware analysis activities; foreign assistance projects; or coordination of cyber assistance efforts with partner countries. The Department of State views such activities as critical to strengthen collective cyber defense and resilience and to help countries resist cyberattacks aimed at coercing them or otherwise interfering with their sovereignty.

Line of Effort 4: Hold Irresponsible States Accountable

To constrain our adversaries effectively and counter malicious activities below the threshold of armed conflict, we will continue to work with our allies and partners to condemn this activity and impose meaningful consequences. These efforts use all the tools of statecraft, including diplomatic isolation, law enforcement, counter-cyber operations, and economic sanctions. In September 2019, 27 countries publicly pledged in a U.S.-led Joint Statement on Advancing Responsible State Behavior in Cyberspace to collaborate voluntarily to hold states accountable when they act contrary to the framework. The number of states willing to publicly hold states accountable reached 39 in July 2021 when NATO, the EU, Australia, Canada, New Zealand, the United Kingdom, and Japan all publicly condemned the PRC's involvement in the Microsoft Exchange server data breach incident and other malicious cyber activities. More recently, likeminded coalitions attributed Russia's cyberattack on Viasat's KA-SAT satellite communications network on the eve of its invasion of Ukraine and stood in solidarity with Albania in the wake of Iran's disruptive cyber operations. The United States will continue to work to expand the coalition of those willing to hold states accountable for disruptive and destabilizing cyber activity and to utilize appropriate multilateral groupings to support each other and to assist the victims of such behavior.

Line of Effort 5: Affirm Application of Mutual Defense Treaties with Certain Allies to the Cyber Domain

In line with the long-standing U.S. recognition that existing international law applies in cyberspace, obligations under treaties and other international agreements may apply in cyberspace. Over the past several years, the United States and certain allies have made public statements affirming the application in cyberspace of obligations in their respective mutual defense treaties, including the 1951 Security Treaty between Australia, New Zealand and the United States (ANZUS) (2011); the North Atlantic Treaty (2014); the Treaty of Mutual Cooperation and Security between the United States and Japan (2019); and the Mutual Defense Treaty between the United States and the Republic of Korea (2023). The Departments of State and Defense will continue to work together with allies to engage in pre-contingency planning and to raise awareness further with alliance partners that existing mutual defense treaties may apply in cyberspace and that cyberattacks rising to the level of an armed attack may trigger mutual defense obligations under such treaties.

Figure 5. The Second International Counter Ransomware Initiative Summit November 2022; Vice President Kamala Harris center left and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger center right with leaders from Australia, Austria, Belgium, Brazil, Bulgaria, Canada, Croatia, Czech Republic, Dominican Republic, Estonia, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, the Netherlands, New

Zealand, Nigeria, Norway, Poland, Republic of Korea, Romania, Singapore, South Africa, Spain, Sweden, Switzerland, United Arab Emirates, United Kingdom, United States, and Ukraine, and the European Union. (U.S. Department of State photo.)

Line of Effort 6: Counter Criminal and Ransomware Actors

For many countries, the greatest risk to their digital security and economies is online scams, criminal hacking, and other financial crimes. Ransomware in particular has emerged in recent years as a clear threat to national security, public safety, and economic prosperity. Operating from safe havens like the PRC, DPRK, Iran, Russia, and certain other countries, ransomware operators have disrupted government services, hospitals, schools, pipeline operations, and civil society entities. With some states using ransomware actors as proxies or turning a blind eye to their activities and the significant impact of their cyberattacks on critical infrastructure, it is increasingly clear that ransomware activity can threaten international peace and security. Digital solidarity is clearly expressed through the Department of State's efforts to leverage its diplomatic capabilities to support the whole-of-government fight against ransomware and other forms of cybercrime, including by building partner capacity; developing coalitions to prevent, disrupt, and punish criminal behavior; and fostering cooperation with the private sector.

The Departments of State, Homeland Security, and Justice will continue to participate in the U.S. Joint Ransomware Task Force and to partner with private industry and international allies to disrupt online criminal infrastructure and resources, take down botnets, and seize cryptocurrency garnered from ransomware campaigns. For example, the U.S. Transnational and High-Tech Crime Global Law Enforcement Network (GLEN) program—a long-standing partnership between the Departments of State and Justice—is a global law enforcement capacity-building network of DOJ International Computer Hacking and Intellectual Property (ICHIP) regional advisors, computer forensic analysts, and federal law enforcement agents. Twelve ICHIP attorney advisors are located around the world. The ICHIP advisor based in The Hague facilitated cooperation among the United States, France, Germany, the Netherlands, the United Kingdom, Romania, and Latvia in the largest ever takedown of the botnet and malware known as Qakbot in August 2023. The network also delivers training and technical assistance to foreign law enforcement partners, prosecutors, and judicial authorities to combat intellectual property theft and cybercrime activity, as well as to assist in the collection and use of electronic evidence to combat all types of crime. The program improves U.S. security by reducing the use of foreign computing infrastructure for malicious activities targeting U.S. networks and by showing that no malicious actor can evade the rule of law.

The GLEN has stood up five regional cryptocurrency working groups around the globe, which are dedicated to information sharing and capacity building to address criminal misuse of cryptocurrency, including in ransomware. Additional priorities for capacity building include Internet fraud and combating the growing scourge of online child sexual exploitation and abuse.

The Department of State will continue to use its diplomatic engagements and capacity building to broaden and strengthen participation in the International Counter Ransomware Initiative (CRI). The CRI is a unique and geographically diverse coalition of nearly 60 countries, plus multilateral institutions such as the European Union, Interpol, and Organization of American States, committed to building collective resilience to ransomware, cooperating to disrupt ransomware and pursue the actors responsible, countering the illicit finance that underpins the ransomware ecosystem, and working with the private sector to defend against ransomware attacks. As a complement to the CRI, the Department of State, in coordination with the U.S. Joint Ransomware Task Force, will continue to develop bilateral and multilateral efforts designed to discourage states from sponsoring ransomware or permitting their territories to be used as safe havens by cyber criminals.

The work of the CRI supports the implementation of the framework for responsible state behavior in cyberspace, including the voluntary norm that "states should respond to appropriate requests for assistance by another state whose critical infrastructures are subject to malicious ICT acts," in addition to "appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty." **[5]**

Line of Effort 7: Safeguard Democratic Processes and Institutions

With more than 70 countries and nearly half the world's population experiencing elections in 2024, their vulnerability to cyber-enabled interference—including potential cyberattacks that disrupt electoral processes; espionage, surveillance, and intimidation of politicians, activists, and journalists; and cyber-enabled malign influence activities that seek to impact election outcomes and undermine public confidence in elections—is particularly acute. The United States has highlighted publicly and in international engagements that it considers election infrastructure to be part of critical infrastructure. It has also noted some states' efforts to use cyber means to destabilize democratic processes. The United States, allies, and partners will continue to expose and defend against malicious operations designed to destabilize

democratic processes and societies, including by sharing threat information and strengthening the resilience of election commissions and other key institutions. The United States, for example, joined a United Kingdom-led effort in 2023 to call out Russia-backed online influence actors and hackers for operations targeting UK politicians and democratic processes. This diplomatic effort was accompanied by the Department of Justice concurrently announcing criminal charges against two of the responsible actors.

Line of Effort 8: Combat the Proliferation and Misuse of Commercial Spyware

The proliferation and misuse of commercial spyware poses a significant threat to both U.S. national security—including counterintelligence interests—and to democratic values and human rights around the globe by enabling the surveillance, repression, and targeting of journalists, human rights defenders, anti-corruption activists, and other civil society members. In March 2023, President Biden signed an executive order limiting U.S. government operational use of commercial spyware that poses significant counterintelligence or security risks to the United States, or significant risks of improper use, including committing human rights abuses, by a foreign government or foreign person. At the same time, the Department of State launched a Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware with 10 other countries committed to undertaking concrete efforts to counter the misuse and proliferation of commercial spyware, which an additional 6 countries joined in March 2024.

Moving forward, the U.S. government will continue to work to disincentivize misuse and positively reshape the commercial spyware market by driving out or encouraging reform by businesses associated with the misuse of these tools. The Department of State will continue to engage diplomatically to urge the countries that have already joined the Joint Statement to take concrete steps to counter the misuse and proliferation of commercial spyware, induce additional countries to join, and persuade countries that misuse or enable the misuse of spyware to implement safeguards to deviate less from U.S. policy. The Department of State will continue to partner with the Departments of Commerce and Treasury to promote accountability for those who misuse—or enable or benefit from the misuse—of commercial spyware through tools like sanctions, visa restrictions, and export controls. In addition, the Department of State will continue to elevate this issue in multilateral and public forums as well as engage closely with civil society, journalists, tech platforms, and the investment community.

ACTION AREA 4: Strengthen and Build International Partner Digital Policy and Cyber Capacity

Digital and cyber capacity building activities are powerful signs of digital solidarity in action. They assist partners build secure, diverse, and resilient ICT infrastructure and grow global markets for interoperable, secure ICT goods and services. They are also critical for emerging economies to achieve the SDGs.

Adversaries, and the PRC in particular, understand this and look to out-match the United States and like-minded partners by offering holistic support for ICT development from full package training programs to higher-level education and scholarships. The Department of State, working with other federal agencies, international allies and partners, and the private sector, seeks to mobilize technology as well as processes and people in support of our partners' economic and development goals. This assistance often has a catalytic effect, encouraging partner countries to prioritize and invest further in cybersecurity and resilience. It also increases understanding of the benefits of the cybersecurity and digital policy approaches advocated by the United States.

In an effort to increase digital solidarity in the realm of foreign assistance, USAID launched the Donor Principles for Human Rights in the Digital Age in partnership with Canada's International Development Research Centre (IDRC), and in collaboration with the Department of State. These principles – endorsed by 38 partner governments – offer a unified framework and set of benchmarks to promote an inclusive, rights-respecting approach to foreign assistance on digital issues.

To achieve our goals, we must work to ensure we can act quickly and effectively in supporting foreign partners' needs for incident response, trusted infrastructure development, and capacity building.

Line of Effort 1: Support and Expand Digital Policy, Legal, and Regulatory Capacity Building Efforts

For digital infrastructure to reach and effectively serve the public, countries need to have the appropriate legal and regulatory frameworks. It is not enough to promote secure, resilient

technology infrastructure; an effective regulatory framework that is transparent, flexible, and technology neutral must be in place to ensure meaningful connectivity. Thus, U.S. foreign assistance focuses on developing and strengthening relevant legislative and regulatory frameworks as well as building local technical capacity and addressing workforce issues.

The Department of State will continue to provide partners the expertise and training they need to develop and govern secure, rights-respecting digital ecosystems. Through technical assistance, ICT and telecom policy capacity building, and training grants, DCCP has facilitated pro-competitive legal and regulatory reforms. For example, Promoting American Approaches to ICT Policy and Regulation (ProICT), another DCCP activity led by the Department of State and USAID , has helped clear the way for new entrants into 5G markets and provided technical advisory support for a 5G spectrum auction.

The Department of State, USAID, NTIA, and FCC, working with industry and the private sector, will continue to provide training programs and technical assistance to developing country officials involved in managing spectrum, deploying wireless and satellite technologies, and acquiring cloud services.

Line of Effort 2: Augment Partner Cyber Capacity Building Efforts

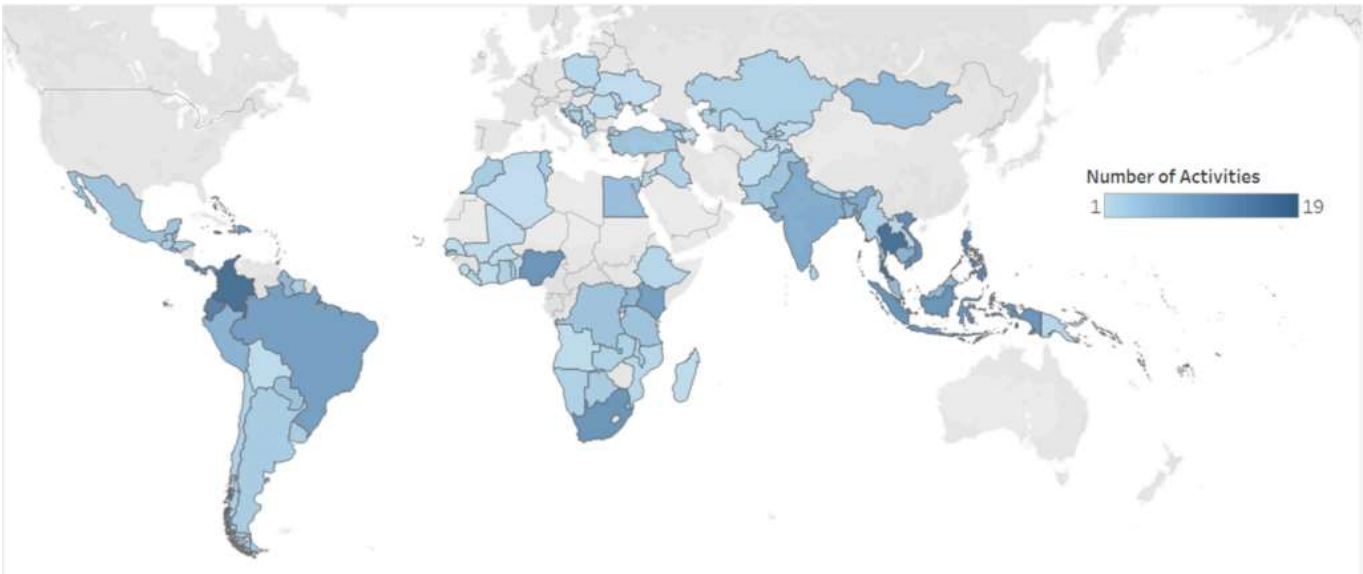

Figure 6. A global map of the Digital Connectivity & Cybersecurity Partnership activities (2018-2024). (U.S. Department of State, CDP)

Cyber capacity building efforts—which usually focus on strengthening a nation's ability to adopt and develop cyber policies and strategies or improving their technical ability to detect, respond to, and recover from cyber incidents—have a direct and positive impact on international cyber stability and the security of U.S. citizens. Assistance directed at policy- and

strategy-making increases states' credibility and engagement in international discussions. It provides them with the national-level capabilities needed to implement the norms developed under the framework for responsible state behavior in cyberspace, to conform with the standards of the Budapest Cybercrime Convention, to hold irresponsible actors accountable in cyberspace, and to develop a national-level approach to counter persistent cyber threats and build long-term resilience. Improving partner operational capabilities makes it more likely they will be able to combat transnational cybercrime threats, share useful cyber threat and incident information with the United States, and successfully partner with the United States in operations to disrupt malicious cyber activity.

Over the last two decades, the Department of State has collaborated with other agencies, international partners, regional organizations, and the private sector to build cyber capacity abroad. Officials and private sector professionals from around the world participate in workshops on industrial control systems held with CISA. The United States assists efforts by the Organization of American States in areas such as cyber incident response, national cybersecurity strategy development and implementation, cybersecurity awareness, and cyber workforce development. The United States is a leading donor to Council of Europe programs designed to expand adoption of the Budapest Cybercrime Convention. The Global Forum on Cyber Expertise (GFCE), of which the United States is a founding and active member, provides a global platform to connect cyber policymakers, practitioners, and experts and to match assistance programs with recipients.

Multiple agencies have supported international partners in using and adapting the NIST Cybersecurity Framework, and the Department of State has supported international participation in the development of version 2.0 of the framework. The NICE Workforce Framework for Cybersecurity (NICE Framework) has been leveraged to support talent development and management. The Department of Commerce, NIST, USAID, and the Department of State will engage international partners to promote the development of critical and emerging technology standards in areas such as best practices regarding data capture, processing, privacy, handling, and analysis; trustworthiness, verification, and assurance of AI systems and AI risk management; and content authentication and provenance, synthetic content detection, and content labeling. In addition, NIST has selected four algorithms designed to withstand cyberattacks by quantum computers and is developing standards for U.S. Government use. The Department of State will work with NIST to internationalize – including through ongoing engagements in international standards bodies – these post quantum cryptography standards so that organizations around the world can integrate them into their encryption infrastructure. They will also continue engaging international partners in developing and implementing cybersecurity best practices in areas

such as Zero Trust, IoT cybersecurity, digital identity, operational technology, software security, and supply chain risk management.

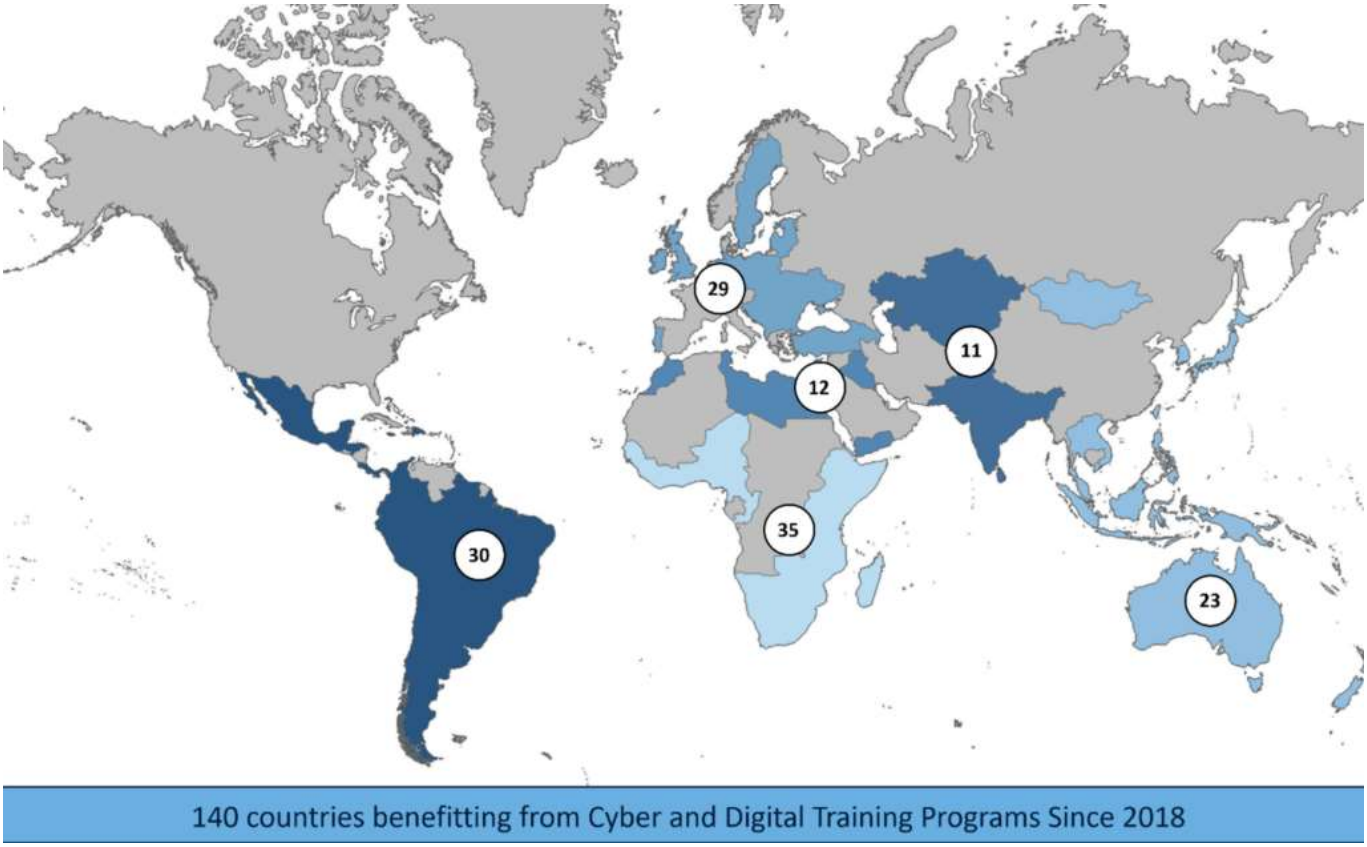

Figure 7. A global map of the Digital Connectivity & Cybersecurity Partnership countries benefitting from Cyber & Digital Training (2018-2024). (U.S. Department of State, CDP)

The Department of State will continue coordinating closely with DoD, DOJ, DHS, CISA, NIST, NTIA, USAID, Department of Treasury, Department of Energy, Department of Commerce, and other federal agencies to help ensure that multiple streams of capacity building feed into and support strategic interests.

Figure 8. (Left) Nathaniel C. Fick U.S. Ambassador at Large for Cyberspace and Digital Policy, (center) Rodrigo Chaves Robles President of Costa Rica, (right) Anne Neuberger Deputy National Security Advisor for Cyber and Emerging Technology at a Center for Strategic and International Studies (CSIS) event on August 30, 2023. (CSIS photo.)

Line of Effort 3: Develop New Tools to Deliver Digital and Cyber Assistance Quickly and Efficiently

The demand for cybersecurity and cybercrime assistance, in particular cyber defense, incident response, and skills to combat criminal misuse of cryptocurrency, is growing in scale. After cyberattacks against Ukraine, Costa Rica, and Albania, the United States and its allies shared threat intelligence; facilitated operational collaboration; enabled access to commercial cybersecurity companies' services, including hardware, software, and embedded technical support; and funded longer term capacity building.

From these and other cases, the State Department has learned the importance of regular and close coordination across the U.S. government and with international partners, as well as the importance of mobilizing private-sector technology and expertise. Modernizing authorities and mechanisms to provide technology-related foreign assistance at the speed and scale necessary is crucial. We must adapt our foreign assistance resources and authorities to support long-term U.S. leadership and foster digital solidarity.

Recognizing the urgent and growing need for additional tools to advance U.S. cyber and digital foreign policy, Congress created, through the Department of State Authorization Act of 2023 and funded, through the Department of State, Foreign Operations, and Related Program Appropriations Act, 2024, the Cyberspace, Digital Connectivity, and Related Technologies Fund. This fund will provide the Department of State with authorities and dedicated funding to support strategically important cyber, digital, and technology-related foreign assistance programs. This is a significant step in advancing U.S. foreign policy. The Department will work to operationalize and implement these new authorities.

Ukraine

The United States, allies, and partners have invested in Ukrainian cyber capacity building for years, providing a foundation for more immediate assistance in mitigating and recovering from attacks. Before Russia's full-scale invasion of Ukraine, U.S. agencies, including the Federal Bureau of Investigation, U.S. Cyber Command, and the Cybersecurity and Infrastructure Security Agency, shared cyber intelligence with Ukrainian partners. Since the invasion, the United States, United Kingdom, and EU Governments have delivered more than $100 million in cyber foreign assistance and enabled Ukrainian agencies to access the services of commercial cybersecurity companies. In 2023, the U.S. and nine close partners established the Tallinn Mechanism, a donor coordination group that aims to deliver assistance quickly and efficiently in support of Ukraine's most urgent cybersecurity needs.

Costa Rica

Following a year of repeated ransomware attacks on Costa Rica's government networks that impacted critical services such as health care, tax collection, and customs, and resulted in a national emergency, the United States announced an $25 million assistance package to address immediate critical cyber

vulnerabilities, including hardware, software, licenses, and embedded technical support. Working with the Costa Rican Ministry of Science, Innovation, Technology, and Telecommunications, the United States helped establish and equip a centralized security operations center to monitor, prevent, detect, investigate, and respond to cyber threats. The United States is also supporting medium- and longer-term technical projects and workforce development to help Costa Rica develop a secure, resilient, and locally sustainable cyber ecosystem.

Albania

In the case of Albania, after a request from the prime minister in July 2022, the U.S. rapidly deployed technical teams in response to a destructive cyberattack, which featured ransomware and wiper malware against public sector networks, including some Albania had designated as critical infrastructure. The U.S. government and the private sector attributed the attack to Iran, and the State Department coordinated a diplomatic campaign that included U.S. sanctions and NATO and EU statements of condemnation. After these more immediate responses, the State Department turned to longer-term capacity building, including implementing over $50 million in U.S. assistance to civilian and military agencies to harden their networks. International partners such as the UK and EU have also provided cybersecurity assistance. U.S. agencies, including the Department of State, Federal Bureau of Investigation, U.S. Cyber Command, and the Cybersecurity and Infrastructure Security Agency continue to collaborate with Albanian cyber authorities following subsequent smaller scale cyberattacks in 2023 and 2024.

Conclusion

As the NSS and NCS note, the 2020s are a decisive decade, and actions taken now will shape the contours of cyberspace, digital technologies, and the digital economy for the future. As it implements this strategy, the Department of State will work with Congress and interagency partners to evaluate current cyber authorities and to amend or create authorities as needed for the Department to keep pace with evolving cyber and digital technologies.

Building innovative, secure, and rights-respecting digital ecosystems is a process that will extend beyond the timespan of this strategy, and likely to be characterized by progress, pauses, and reversals. There will be, however, some early signposts that will indicate the United States, allies, and partners are moving forward.

First, the United States, allies, and partners, along with the private sector and civil society, will build on the early successes of the G7-Hiroshima Code of Conduct, the Biden-Harris Executive Order on AI, and the UK AI Safety Summit. We will reach consensus on guiding principles that foster innovation and the development of responsible AI as well as make significant investments to build the knowledge and infrastructure necessary to measure, evaluate, and verify advanced AI systems, including through the launch of the U.S. AI Safety Institute. We will advance global norms on the responsible and rights-respecting use of AI-enabled technologies.

Second, the United States allies, and partners, along with the private sector, will develop common understandings and shared principles for security and trustworthiness in subsea cable, cloud services, and data centers and will increase support for extending access to cloud services to emerging economies.

Third, the United States, allies, and partners will succeed in pushing forward more action-oriented discussions at the UN on international security issues in cyberspace. These discussions will focus on how member states can work together to implement critical elements of the framework for responsible state behavior and on building all states' capacity to manage cyber-related threats.

Fourth, the Department of State will draw on the Cyberspace, Digital Connectivity, and Related Technologies Fund to provide rapid incident response and cyber aid quickly and effectively, as well as longer-term capacity and resilience building. These strategic investments will not only strengthen the role of the United States as a digital partner, but also generate larger, self-sustaining investments by host countries in their own cybersecurity and digital transformation.

Moving forward, the United States will strive for a future in which cyberspace and digital technologies are used to advance economic prosperity and inclusion, enhance security, promote and protect human rights and democracy, and address transnational challenges. The Department of State will build and extend digital solidarity to partners across the globe. The United States recognizes the need to work together to align approaches to data and digital governance and to promote the research, development, and deployment of critical and emerging technologies. The United States seeks to be the partner of choice in improving cybersecurity, building resilience, responding to, and recovering from malicious cyber activity. Digital solidarity aims to connect people and information like never before, fostering a more inclusive, secure, prosperous, rights-respecting, safe, and equitable world.

. . .

Notes

[1] The idea of digital solidarity was first promoted by Pablo Chavez, "Toward Digital Solidarity," Lawfare, June 28, 2022, **https://www.lawfaremedia.org/article/toward-digital-solidarity** **[back to 1]**

[2] Fast Track Action Subcommittee on Critical and Emerging Technologies, Critical and Emerging Technologies Update, National Science and Technology Council, February 2024, **https://www.whitehouse.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf**
[back to 2]

[3] Anna Fleck, "Cybercrime Expected To Skyrocket in Coming Years," Statista, February 22, 2024, **https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/** **[back to 3]**

[4] ITU, The Gender Digital Divide, **https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-the-gender-digital-divide/** **[back to 4]**

[5] UN, Secretary General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, July 2015, **https://digitallibrary.un.org/record/799853?ln=en&v=pdf** **[back to 5]**

TAGS

Bureau of Cyberspace and Digital Policy | Cyber Issues | Cyber Security