Attachment #8

The Cyber Social Contract

By Chris Inglis and Harry Krejsa
February 21, 2022

In the spring of 2021, a Russia-based cybercrime group launched a ransomware attack against the largest fuel pipeline in the United States. According to the cybersecurity firm Mandiant, the subsequent shutdown and gas shortage across the East Coast likely originated from a single compromised password. That an individual misstep might disrupt critical services for millions illustrates just how vulnerable the United States' digital ecosystem is in the twenty-first century.

Although most participants in the cyber-ecosystem are aware of these growing risks, the responsibility for mitigating systemic hazards is poorly distributed. Cyber-professionals and policymakers are too often motivated more by a fear of risk than by an aspiration to realize cyberspace's full potential. Exacerbating this dynamic is a decades-old tendency among the large and sophisticated actors who design, construct, and operate digital systems to devolve the cost and difficulty of risk mitigation onto users who often lack the resources and expertise to address them.

Too often, this state of affairs produces digital ecosystems where private information is easily accessible, predatory technology is inexpensive, and momentary lapses in vigilance can snowball into a continent-wide catastrophe. Although individually oriented tools like multifactor authentication and password managers are critical to solving elements of this problem, they are inadequate on their own. A durable solution must involve moving away from the tendency to charge isolated individuals, small businesses, and local governments with shouldering absurd levels of risk. Those more capable of carrying the load—such as governments and large firms—must take on some of the burden, and collective, collaborative defense needs to replace atomized and divided efforts. Until then, the problem will always look like someone else's to solve.

The United States needs a new social contract for the digital age—one that meaningfully alters the relationship between public and private sectors and proposes a new set of obligations for each. Such a shift is momentous but not without precedent. From the Pure Food and Drug Act of 1906 to the Clean Air Act of 1963 and the public-private revolution in airline safety in the 1990s, the United States has made important adjustments following profound changes in the economy and technology.

A similarly innovative shift in the cyber-realm will likely require an intense process of development and iteration. Still, its contours are already clear: the private sector must prioritize long-term investments in a digital ecosystem that equitably distributes the burden of cyberdefense. Government, in turn, must provide more timely and comprehensive threat information while simultaneously treating industry as a vital partner. Finally, both the public and private sectors must commit to moving toward true collaboration—contributing resources, attention, expertise, and people toward institutions designed to prevent, counter, and recover from cyber-incidents.

Although success is far from guaranteed, the benefits of such a social contract are enormous. A new vision of what the U.S. government, firms, and individuals owe one another in cyberspace—unburdened by contemporary visions of risk and threat—ultimately means a world capable of achieving its full technological potential.

A DREAM DEFERRED

Contemporary cyberthreats represent a tragic betrayal of what leading technology advocates promised at the dawn of the digital revolution. The heady early days of the Internet were suffused with optimism. Digital connectivity, many argued, would not only favor democracy and human rights but would also serve as an inherent force of progress and egalitarianism. After the fall of the Soviet Union in the early 1990s, it was easy to see the Internet as a natural and inevitable extension of liberalizing geopolitical forces—heralding a world where neither physical borders nor governmental authorities would constrain the free flow of ideas.

It soon became clear, however, that cyberspace was a tool like any other—one that would amplify the values of those who wielded it. China, initially held up as a quintessential case of liberalization-by-commerce, did precisely what techno-optimists thought impossible: it tamed the Internet, harnessed cyberspace, and subverted the digital revolution into a digital dystopia that Beijing now seeks to export to aspiring authoritarians worldwide. Russia, whose Soviet forebears were partly defeated by the free flow of information, is now a virtuosic purveyor of disinformation, digital manipulation, and cyber-enabled geopolitical blackmail.

Individuals and small businesses, meanwhile, have only partially realized the promise of a radically egalitarian digital economy. Market gains have disproportionately accrued to a few large firms. The digital criminal underground, by contrast, is far more democratic. Hacking tools are readily available, enabling cybercriminals to hold critical infrastructure hostage. The digital hopes of the 1990s are now interlaced with a series of catastrophic threats.

With that backdrop, it should come as no surprise that many cyberpolicies proceed from a fundamentally negative framing that cedes the initiative to transgressors and places excessive faith in market incentives. There is merit to these concerns: the security challenges in cyberspace are daunting because the scope and scale of any one security incident can be so vast. In a world where clicking the wrong link or neglecting a single software patch can result in a geopolitical incident, responders often focus on an attack’s perpetrator at the expense of addressing the perverse incentives that create these circumstances in the first place. Such framing has serious material consequences, however. Security is a prerequisite for prosperity in the physical world, and cyberspace is no different. Until Washington develops a better understanding of what digitally enabled prosperity might look like, the United States will continue to miss out on cyberspace’s original purpose: the ambitious realization of a better world, a more equitable economy, and a more just society.

A NEW SOCIAL CONTRACT

Neither market incentives nor existing threats are immutable forces of nature. Change is possible, and it is wholly consistent with American values for government to collaborate with the

Attachment #8

private sector to mitigate risk and better serve public interests. The best way to begin this reset is by increasing collaboration within the U.S. government and—perhaps most importantly—creating a clear framework for collaboration across the public and private elements of the United States' shared cyber-ecosystem.

The U.S. government has made great strides in the former. The Biden administration has unveiled a series of whole-of-government initiatives meant to apprehend criminals, isolate and sanction their enablers, and mobilize like-minded states to defend against state-backed hacking campaigns. Across the public and private sector, however, there remains little common understanding of what an organization ought to do or to whom it should turn when preparing for or responding to an intrusion. Governments, firms, and citizens alike too often have no authoritative answer to the question of what we owe one another in cyberspace.

The answer to that question requires collaboration among the U.S. government, the private sector, and their international counterparts. Situational awareness—the kind needed to understand threats that operate across organizational boundaries—is only possible if each organization contributes its fractional views to a shared understanding of a common threat. Collaboration between cyber defenders can turn the tables on attackers, but only if every stakeholder understands how their part fits into the whole and under what circumstances they must be ready to step in to help.

The United States needs a new social contract for the digital age.

As in other industries charged with providing critical services, however, market forces alone are insufficient to ensure that cyberspace serves all of its stakeholders equitably. Consistent with best practices derived from the transportation and medical sectors, government and private firms must begin to work together. Above all, that means developing new ways to address the disproportionate burden that the current system places on individuals and end users. Cyberspace is made up of overwhelmingly private components yet has incalculable public value. Private sector firms will, therefore, need to increasingly prioritize security and resilience in both their hardware manufacturing and software development, even if those priorities require more patience from their occasionally impatient investors. The government must also play an active role in easing that transition—setting standards, incentivizing norms, and providing information.

Both sides also need to match these actions with a novel vision for collaboration. Building resilience to potentially catastrophic cyber-incidents will require an unprecedented level of planning, information sharing, and operational intimacy across once-isolated fields. Existing efforts to place government and industry experts side-by-side—including in sector-specific Information Sharing and Analysis Centers—are a good way to start. The U.S. government has quickly realized that these partnerships can identify and address threats far more effectively than a single organization operating alone.

President Joe Biden's May 2021 executive order on improving U.S. cybersecurity is a vital element of this new paradigm. The order is designed to foster resilient software supply chains by strengthening information technology standards and defending networks against known vulnerabilities. Security researchers have long called for many of the order's new initiatives,

Attachment #8

including a so-called software bill of materials program designed to track various components used in software development. Biden's announcement, moreover, will help disseminate these practices well beyond the public sector alone.

The federal government will also need to lead by example when building its own digital systems. In November 2021, the Cybersecurity and Infrastructure Security Agency (CISA) issued a novel directive requiring all federal agencies to patch more than 250 known software vulnerabilities that hackers were actively exploiting. In January 2022, the administration unveiled its strategy for implementing a government-wide zero-trust architecture—a security philosophy that assumes breaches are inevitable and builds in firebreaks to contain the impact of any potential hack. Such a program lowers the risk of any single vulnerability, moving the United States away from a system that too often concentrates risk on individuals' digital slip-ups. Beyond simply urging a change of direction and strategy, the federal government is getting its own digital house in order and blazing a path that others can follow.

Cyberthreats represent a betrayal of what advocates promised at the dawn of the digital revolution.

Translating this level of mobilization into systemic change across the private sector will be a more difficult proposition. Doing so will require an unprecedented level of collaboration between government and industry. As a start, the Biden administration is setting up a new Cyber Safety Review Board modeled after the National Transportation Safety Board. Government and private sector leaders will co-chair this body with an intent to analyze significant cybersecurity incidents, generate lessons learned, and produce concrete recommendations to avoid future crises. Washington is also easing contractual barriers that once prevented private sector actors from sharing threat information with authorities and requiring government service providers to notify federal agencies of relevant data breaches. Finally, the Biden administration established the Joint Cyber Defense Collaborative at CISA, a first-of-its-kind organization with authority to bring together representatives from government and industry to identify threats, develop crisis response plans, and foster the relationships needed to respond to malicious cyber-incidents.

This level of collaboration will require professional and operational intimacy among practitioners and considerable experience in developing plans for exceptional events. CISA, for instance, will need to convene whole-of-nation exercises designed to anticipate particular contingencies and identify the agencies responsible for specific elements of crisis response. CISA and its fellow risk management agencies across the rest of the federal government will also need to carry out their responsibilities alongside their counterpart industries. Private and public sector leaders will need to learn how to speak one another's languages and productively share information. And the National Security Council will need to coordinate the deployment of all tools of national power when a cyber problem suddenly becomes a geopolitical problem.

Like any well-functioning team, however, the U.S. government also needs to regularly review its performance. This is another area where the Office of the National Cyber Director (ONCD) can prove its worth. From its position in the White House, ONCD must use its perspective to champion and drive coherence across U.S. cyber policy. That should include carefully reviewing budgets to identify effective policies and translating national strategies into planning priorities for specific agencies. ONCD must also identify weaknesses in Washington's crash course in public-private cooperation and repair organizational issues before they become serious problems. Cyberspace is the world's largest public good composed almost entirely of private components, and ONCD, armed with its statutory responsibility to consult and coordinate with private sector actors, must work as the government's translator. Finally, because cyberspace is not a purely domestic issue, ONCD should work alongside the State Department and National Security Council to ensure that lessons learned flow freely between the United States and its partners.

PRESENT AT THE CREATION

With this new social contract for cyberspace—based around investments in resilience, new forms of information sharing, and public-private collaboration—the United States will be well placed to reclaim the hope present at the dawn of the digital age. Although Americans have grown skeptical that the Internet is a net positive development for society, unrealized promise abounds at the intersection of public and private collaboration. By revamping its understanding of whom and what cyberspace is ultimately for, the United States will be poised to reap untold social, economic, and geopolitical benefits.

The tech sector, for one, is already a significant engine of innovation and growth—constituting nearly ten percent of the United States' total economic output. Seven of the ten most profitable U.S. companies are technology, telecommunications, or software firms. Eighty-five percent of Americans own a smartphone, up from 35 percent just ten years ago—a signal of just how deeply digital connectivity is woven into the fabric of American life. And when COVID-19 arrived, 90 percent of Americans said the Internet became essential or important to weathering the unprecedented disruption brought by a global pandemic.

Digital connectivity is not only helping individuals cope with COVID-19, however. Technology is also assisting governments, scientists, and companies to manage and ultimately end the pandemic. Since 2020, a historic global mobilization of biomedical research has transformed science in the digital age. COVID-19 researchers piloted new practices for rapidly sharing data and results—frequently circulating so-called preprint papers to disseminate vital discoveries all while maintaining data security and integrity. When scientists first sequenced an early version of the SARS-CoV-2 viral genome in January 2020, for instance, researchers at the biotechnology firm Moderna and the U.S. National Institute of Allergy and Infectious Diseases simply downloaded the genome, swapped out one viral protein for another, and began testing a vaccine within six weeks.

Aligning market incentives to realize a low-carbon future requires attention and creativity.

Vitally, this newfound speed did not entail sacrifices in quality. Instead, digital connectivity helped strengthen medical science's ethical, doctrinal, and procedural underpinnings, allowing it to operate at higher speeds without sacrificing public safety. The protections and controls that researchers built into every layer of their work—how they designed their experiments, collected and handled their data, selected and operated their tools and materials—created layers of risk mitigation that produced a faster and higher-performing industry. Although the international community still faces political hurdles to vaccinating the most vulnerable, the public now understands what is truly possible.

Beyond issues such as COVID-19, however, the United States has scarcely begun to imagine what a similar high-performance, high-confidence framework—with significant safeguards built into its design—could accomplish in other fields. As with biomedical research, the policies, processes, and technologies necessary for a stable and secure Internet are not a drag on speed but actually allow innovators to unfurl their initiatives more quickly and confidently. The United States should therefore develop its cyber strategies, policies, and partnerships not by solely fixating on the most imminent threats but by remembering the promise that lies ahead. By more clearly articulating the digitally enabled world where Americans want to live, the path forward will become increasingly achievable.

A BRIGHT FUTURE

It is impossible to predict what an ideal digital and collaborative future might look like, but its broad benefits are increasingly visible. Some elements that hold clear promise when paired with a newly secure and durable digital ecosystem already exist. Others are more speculative. In all cases, however, a world where scientists, innovators, governments, and individuals have the confidence to move faster in cyberspace is one where the future is bright.

One of the most promising and urgent possibilities involves the transition to renewable energy. Although the Biden administration's once-in-a-generation Infrastructure Investment and Jobs Act investments will accelerate this movement, the promise of renewable energy is about more than just slowing climate change. Green energy can ultimately enable a more ambitious and compelling future than fossil fuels could ever provide. U.S. per capita energy use grew rapidly as the United States industrialized but plateaued after the 1970s as rising oil prices and pollution drove industry to do more with less. The cost of solar panels, meanwhile, has declined rapidly—more than 80 percent since 2010. When combined with the near-zero marginal cost of converting sunlight to electricity, energy may soon become too cheap to meter. Analysts have barely begun to imagine what a U.S. economy unchained from energy scarcity and pollution could accomplish.

Aligning market incentives to realize this low-carbon future requires attention and creativity. The same is true for the secure and resilient digital foundation that such a system would ultimately utilize. Solar energy, for example, is uniquely scalable—from the rooftops of individual homes to utility-scale solar farms. Designed correctly, the digital infrastructure underpinning this hypothetical energy network could generate, store, and redistribute electricity at a level contemporary fossil fuels simply cannot match. With ironclad data security, operators could trust automated software to distribute power with an unprecedented level of sophistication. Southern sunshine could backstop Iowans staring down winter storms, while offshore winds in Maine could charge electric vehicles up and down the East Coast.

Also promising and similarly urgent is the rapidly developing space-based economy. Like renewable energy, this new sector will hinge on cybersecurity and technology security. Orbital launch costs are declining, and satellite technology is increasingly available—opening up new

Attachment #8

opportunities for commercial and geopolitical competition alike. Although space-based telecommunication systems already exist, businesses, governments, nonprofits, and researchers alike need confidence in the security and resilience of the orbital investments they make and the data those systems provide. Precise climate change models, game-changing agricultural insights, real-time measurements of macroeconomic trends, and worldwide Internet connectivity may be just around the corner, but only if the hardware and software that provide these services remain trustworthy, resilient, and operational. This will only happen once the United States reaches an entirely different level of confidence in its cybersecurity underpinnings. As any motorsports fan knows, drivers can take corners faster when they have confidence in their brakes.

By identifying the digital future the United States wants to create, Americans can fortify their resilience.

Autonomous vehicles may be one such technology. The promise of vehicle autonomy is clear: safer and easier transportation of people and goods, reduced driver fatigue, vastly more efficient use of passenger and freight networks, and improved freedom of movement for the disabled or displaced. The threats posed by an insecure cyber-ecosystem, however, are equally clear: autonomous fleets will inevitably depend on densely networked systems and software guidance that are currently vulnerable to malicious attacks. The uniquely real-time and high-stakes use of artificial intelligence that truly autonomous vehicles would require necessitates paradigm-shifting cyber-protections. Once realized, these developments could usher in the most profound and positive change to the modern world's built environment in decades.

Such bright futures also extend into geopolitics. Just as analysts often fixate on cyberthreats to the detriment of cyber benefits, the implications of a future where the United States prevails over contemporary geopolitical threats are similarly understudied. A world in which U.S. and allied networks are resilient against state-backed hacking campaigns, for instance, would be a profoundly different one. If China or Russia had fewer plausible avenues for subverting the digital infrastructure that underpins the United States' conventional tools of deterrence, the calculus of strategic competition would likely shift significantly in favor of the United States. The United States would also stand to benefit if China and Russia were prevented from prepositioning malware in critical U.S. infrastructure, thereby decreasing Beijing and Moscow's ability to wield asymmetric weapons in a crisis.

And although the U.S. public is broadly aware of Chinese espionage and intellectual property theft, analysts are comparatively less aware of Beijing's growing ability to weaponize Americans' individual data. According to William Evanina, former director of the National Counterintelligence and Security Center, China has "vacuumed up the personal data of much of the American population, including data on our health, finances, travel and other sensitive information." China is almost certainly using these vast datasets to develop models for an array of nefarious purposes, including identifying intelligence agents, stymying U.S. diplomacy, tracking influential leaders, targeting Beijing's espionage campaigns, and even influencing voters. Individuals' personal data is not only the lifeblood of the digital economy, it also fuels the weapons that target that economy. A durable and secure digital ecosystem, by contrast, would short-circuit such malign activity.

Attachment #8

Finally, a world where data is more secure is a world where data privacy becomes more enforceable. Americans are increasingly confused and anxious over the lack of control over their personal information, and the regular drumbeat of mass breaches does little to soothe their nerves. By contrast, an absolutely secure digital world is one where a comprehensive privacy regime becomes more practical. With greater certainty over the direction of the United States' data security and privacy environment, U.S. firms would also find it easier to work with the data regimes of like-minded partners. Such collaboration would enable deeper interoperability and commercial exchange with countries such as Japan or those in the European Union that have already begun laying the foundations of twenty-first-century data law. U.S. diplomats would also be able to credibly wield these values as foreign policy tools to strengthen relations with allies and partners across the globe. The resulting international ties would help constrain the spread of Beijing and Moscow's surveillance technologies and digital authoritarianism.

These futures may be rosy, but they are not implausible. By focusing Washington's attention on realizing a preferred digital future, the United States will not only be able to identify malign actors seeking to obstruct U.S. success, it will also be able to generate a more actionable understanding of what Americans need from one another. Many digitally driven sectors have become victims of their own success. Over the past few decades, a series of small and innovative firms have become custodians of a vital new establishment. Rarely is there a clear tipping point when a startup's mission transitions from creative destruction to societal maintenance. But with a shared and affirmative vision, the public and private sectors can build a new social contract that facilitates that transition without undermining the integrity and vitality essential to an innovative economy.

By identifying the digital future the United States wants to create and the social contract that could sustain it, Americans can fortify their resilience and establish rewards for good behavior and costs for bad behavior. Misaligned incentives and malicious actors are no match for a clear vision of where the United States wants to go.