FOREIGN AFFAIRS

A World Without Trust

The Insidious Cyberthreat

BY JACQUELYN SCHNEIDER **January/February 2022**
JACQUELYN SCHNEIDER is a Hoover Fellow at the Hoover Institution at Stanford University.

When sounding the alarm over cyberthreats, policymakers and analysts have typically employed a vocabulary of conflict and catastrophe. As early as 2001, James Adams, a co-founder of the cybersecurity firm iDefense, warned in these pages that cyberspace was “a new international battlefield,” where future military campaigns would be won or lost. In subsequent years, U.S. defense officials warned of a “cyber–Pearl Harbor,” in the words of then Defense Secretary Leon Panetta, and a “cyber 9/11,” according to then Homeland Security Secretary Janet Napolitano. In 2015, James Clapper, then the director of national intelligence, said the United States must prepare for a “cyber Armageddon” but acknowledged it was not the most likely scenario. In response to the threat, officials argued that cyberspace should be understood as a “domain” of conflict, with “key terrain” that the United States needed to take or defend.

The 20 years since Adams’s warning have revealed that cyberthreats and cyberattacks are hugely consequential—but not in the way most predictions suggested. Spying and theft in cyberspace have garnered peta-, exa-, even zettabytes of sensitive and proprietary data. Cyber-enabled information operations have threatened elections and incited mass social movements. Cyberattacks on businesses have cost hundreds of billions of dollars. But while the cyberthreat is real and growing, expectations that cyberattacks would create large-scale physical effects akin to those caused by surprise bombings on U.S. soil, or that they would hurtle states into violent conflict, or even that what happened in the domain of cyberspace would define who won or lost on the battlefield haven’t been borne out. In trying to analogize the cyberthreat to the world of physical warfare, policymakers missed the far more insidious danger that cyber-operations pose: how they erode the trust people place in markets, governments, and even national power.

Correctly diagnosing the threat is essential, in part because it shapes how states invest in cybersecurity. Focusing on single, potentially catastrophic events, and thinking mostly about the possible physical effects of cyberattacks, unduly prioritizes capabilities that will protect against “the big one”: large-scale responses to disastrous cyberattacks, offensive measures that produce physical violence, or punishments only for the kinds of attacks that cross a strategic threshold. Such capabilities and responses are mostly ineffective at protecting against the way cyberattacks undermine the trust that undergirds modern economies, societies, governments, and militaries.

If trust is what’s at stake—and it has already been deeply eroded—then the steps states must take to survive and operate in this new world are different. The solution to a “cyber–Pearl Harbor” is to do everything possible to ensure it doesn’t happen, but the way to retain trust in a digital world despite the inevitability of cyberattacks is to build resilience and thereby promote confidence in today’s systems of commerce, governance, military power, and international cooperation. States can develop this resilience by restoring links between humans and within networks, by strategically distributing analog systems where needed, and by investing in processes that allow for manual and human intervention. The key to success in cyberspace over the long term is not finding a way to defeat all cyberattacks but learning how to survive despite the disruption and destruction they cause.

The United States has not so far experienced a “cyber 9/11,” and a cyberattack that causes immediate catastrophic physical effects isn’t likely in the future, either. But Americans’ trust in their government, their institutions, and even their fellow citizens is declining rapidly—weakening the very foundations of society. Cyberattacks prey on these weak points, sowing distrust in information, creating confusion and anxiety, and exacerbating hatred and misinformation. As people’s digital dependencies grow and the links among technologies, people, and institutions become more tenuous, this cyberthreat to trust will only become more existential. It is this creeping dystopian future that policymakers should worry about—and do everything possible to avert.

THE TIES THAT BIND

Trust, defined as “the firm belief in the reliability, truth, ability, or strength of someone or something,” plays a central role in economies, societies, and the international system. It allows individuals, organizations, and states to delegate tasks or responsibilities, thereby freeing up time and resources to accomplish other jobs, or to cooperate instead of acting alone. It is the glue that allows complex relationships to survive—permitting markets to become more complex, governance to extend over a broader population or set of issues, and states to trade, cooperate, and exist within more complicated alliance relationships. “Extensions of trust . . . enable coordination of actions over large domains of space and time, which in turn permits the benefits of more complex, differentiated, and diverse societies,” explains the political scientist Mark Warren.

Those extensions of trust have played an essential role in human progress across all dimensions. Primitive, isolated, and autocratic societies function with what sociologists call “particularized trust”—a trust of only known others. Modern and interconnected states require what’s called “generalized trust,” which extends beyond known circles and allows actors to delegate trust relationships to individuals, organizations, and processes with whom the truster is not intimately familiar. Particularized trust leads to allegiance within small groups, distrust of others, and wariness of unfamiliar processes or institutions; generalized trust enables complicated market interactions, community involvement, and trade and cooperation among states.

The modern market, for example, could not exist without the trust that allows for the delegation of responsibility to another entity. People trust that currencies have value, that banks can secure and safeguard assets, and that IOUs in the form of checks, credit cards, or loans will be fulfilled. When individuals and entities have trust in a financial system, wages, profits, and employment increase. Trust in laws about property rights facilitates trade and economic prosperity. The digital economy makes this generalized trust even more important. No longer do people deposit gold in a bank vault. Instead, modern economies consist of complicated sets of digital transactions in which users must trust not only that banks are securing and safeguarding their assets but also that the digital medium—a series of ones and zeros linked together in code—translates to an actual value that can be used to buy goods and services.

Trust is a basic ingredient of social capital—the shared norms and interconnected networks that, as the political scientist Robert Putnam has famously argued, lead to more peaceful and prosperous communities. The generalized trust at the heart of social capital allows voters to delegate responsibility to proxies and institutions to represent their interests. Voters must trust that a representative will promote their interests, that votes will be logged and counted properly, and that the institutions that write and uphold laws will do so fairly.

Finally, trust is at the heart of how states generate national power and, ultimately, how they interact within the international system. It allows civilian heads of state to delegate command of armed forces to military leaders and enables those military leaders to execute decentralized control of lower-level military operations and tactics. States characterized by civil-military distrust are less likely to win wars, partly because of how trust affects a regime’s willingness to give control to lower levels of military units in warfare. For example, the political scientist Caitlin Talmadge notes how Saddam Hussein’s efforts to coup-proof his military through the frequent cycling of officers through assignments, the restriction of foreign travel and training, and perverse regime loyalty promotion incentives handicapped the otherwise well-equipped Iraqi military. Trust also enables militaries to experiment and train with new technologies, making them more likely to innovate and develop revolutionary advancements in military power.

Trust also dictates the stability of the international system. States rely on it to build trade and arms control agreements and, most important, to feel confident that other states will not launch a surprise attack or invasion. It enables international cooperation and thwarts arms races by creating the conditions to share information—thus defeating the suboptimal outcome of a prisoner’s dilemma, wherein states choose conflict because they are unable to share the information required for cooperation. The Russian proverb “*Doveryai, no proveryai*”—“Trust, but verify”—has guided arms control negotiations and agreements since the Cold War.

In short, the world today is more dependent on trust than ever before. This is, in large part, because of the way information and digital technologies have proliferated across modern economies, societies, governments, and militaries, their virtual nature amplifying the role that trust plays in daily activities. This occurs in a few ways. First, the rise of automation and autonomous technologies—whether in traffic systems, financial markets, health care, or military weapons—necessitates a delegation of trust whereby the user is trusting that the machine can accomplish a task safely and appropriately. Second, digital information requires the user to trust that data are stored in the right place, that their values are what the user believes them to be, and that the data won’t be manipulated. Additionally, digital social media platforms create new trust dynamics around identity, privacy, and validity. How do you trust the creators of information or that your social interactions are with an actual person? How do you trust that the information you provide others will be kept private? These are relatively complex relationships with trust, all the result of users’ dependence on digital technologies and information in the modern world.

SUSPICION SPREADS

All the trust that is needed to carry out these online interactions and exchanges creates an enormous target. In the most dramatic way, cyber-operations generate distrust in how or whether a system operates. For instance, an exploit, which is a cyberattack that takes advantage of a security flaw in a computer system, can hack and control a pacemaker, causing distrust on the part of the patient using the device. Or a microchip backdoor can allow bad actors to access smart weapons, sowing distrust about who is in control of those weapons. Cyber-operations can lead to distrust in the integrity of data or the algorithms that make sense of data. Are voter logs accurate? Is that artificial-intelligence-enabled strategic warning system showing a real missile launch, or is it a blip in the computer code? Additionally, operating in a digital world can produce distrust in ownership or control of information: Are your photos private? Is your company’s intellectual property secure? Did government secrets about nuclear weapons make it into an adversary’s hands? Finally, cyber-operations create distrust by manipulating social networks and relationships and ultimately deteriorating social capital. Online personas, bots, and disinformation campaigns all complicate whether individuals can trust both information and one another. All these cyberthreats have implications that can erode the foundations on which markets, societies, governments, and the international system were built.

The digitally dependent economy is particularly vulnerable to degradations of trust. As the modern market has become more interconnected online, cyberthreats have grown more sophisticated and ubiquitous. Yearly estimates of the total economic cost of cyberattacks range from hundreds of billions to trillions of dollars. But it isn’t the financial cost of these attacks alone that threatens the modern economy. Instead, it is how these persistent attacks create distrust in the integrity of the system as a whole.

Nowhere was this more evident than in the public’s response to the ransomware attack on the American oil provider Colonial Pipeline. In May 2021, a criminal gang known as DarkSide shut down the pipeline, which provides about 45 percent of the fuel to the East Coast of the United States, and demanded a ransom, which the company ultimately paid. Despite the limited impact of the attack on the company’s ability to provide oil to its customers, people panicked and flocked to gas stations with oil tanks and plastic bags to stock up on gas, leading to an artificial shortage at the pump. This kind of distrust, and the chaos it causes, threatens the foundations not just of the digital economy but also of the entire economy.

The inability to safeguard intellectual property from cybertheft is similarly consequential. The practice of stealing intellectual property or trade secrets by hacking into a company’s network and taking sensitive data has become a lucrative criminal enterprise—one that states including China and North Korea use to catch up with the United States and other countries that have the most innovative technology. North Korea famously hacked the pharmaceutical company Pfizer in an attempt to steal its COVID-19 vaccine technology, and Chinese exfiltrations of U.S. defense industrial base research has led to copycat technological advances in aircraft and missile development. The more extensive and sophisticated such attacks become, the less companies can trust that their investments in research and development will lead to profit—ultimately destroying knowledge-based economies. And nowhere are the threats to trust more existential than in online banking. If users no longer trust that their digital data and their money can be safeguarded, then the entire complicated modern financial system could collapse. Perversely, the turn toward cryptocurrencies, most of which are not backed by government guarantees, makes trust in the value of digital information all the more critical.

Societies and governments are also vulnerable to attacks on trust. Schools, courts, and municipal governments have all become ransomware targets—whereby systems are taken offline or rendered useless until the victim pays up. In the cross hairs are virtual classrooms, access to judicial records, and local emergency services. And while the immediate impact of these attacks can temporarily degrade some governance and social functions, the greater danger is that over the long term, a lack of faith in the integrity of data stored by governments—whether marriage records, birth certificates, criminal records, or property divisions—can erode trust in the basic functions of a society. Democracy’s reliance on information and social capital to build trust in institutions has proved remarkably vulnerable to cyber-enabled information operations. State-sponsored campaigns that provoke questions about the integrity of governance data (such as vote tallies) or that fracture communities into small groups of particularized trust give rise to the kind of forces that foment civil unrest and threaten democracy.

Cyber-operations can also jeopardize military power, by attacking trust in modern weapons. With the rise of digital capabilities, starting with the microprocessor, states began to rely on smart weapons, networked sensors, and autonomous platforms for their militaries. As those militaries became more digitally capable, they also became susceptible to cyber-operations that threatened the reliability and functionality of these smart weapons systems. Whereas a previous focus on cyberthreats fixated on how cyber-operations could act like a bomb, the true danger occurs when cyberattacks make it difficult to trust that actual bombs will work as expected. As militaries move farther away from the battlefield through remote operations and commanders delegate responsibility to autonomous systems, this trust becomes all the more important. Can militaries have faith that cyberattacks on autonomous systems will not render them ineffective or, worse, cause fratricide or kill civilians? Furthermore, for highly networked militaries (such as that of the United States), lessons taken from the early information age led to doctrines, campaigns, and weapons that rely on complex distributions of information. Absent trust in information or the means by which it is being disseminated, militaries will be stymied—awaiting new orders, unsure of how to proceed.

Together, these factors threaten the fragile systems of trust that facilitate peace and stability within the international system. They make trade less likely, arms control more difficult, and states more uncertain about one another’s intentions. The introduction of cybertools for spying, attacks, and theft has only exacerbated the effects of distrust. Offensive cyber-capabilities are difficult to monitor, and the lack of norms about the appropriate uses of cyber-operations makes it difficult for states to trust that others will use restraint. Are Russian hackers exploring U.S. power networks to launch an imminent cyberattack, or are they merely probing for vulnerabilities, with no future plans to use them? Are U.S. “defend forward” cyber-operations truly to prevent attacks on U.S. networks or instead a guise to justify offensive cyberattacks on Chinese or Russian command-and-control systems? Meanwhile, the use of mercenaries, intermediaries, and gray-zone operations in cyberspace makes attribution and determining intent harder, further threatening trust and cooperation in the international system. For example, Israeli spyware aiding Saudi government efforts to repress dissent, off-duty Chinese military hacktivists, criminal organizations the Russian state allows but does not officially sponsor—all make it difficult to establish a clear chain of attribution for an intentional state action. Such intermediaries also threaten the usefulness of official agreements among states about what is appropriate behavior in cyberspace.

LIVING WITH FAILURE

To date, U.S. solutions to dangers in cyberspace have focused on the cyberspace part of the question—deterring, defending against, and defeating cyberthreats as they attack their targets. But these cyber-focused strategies have struggled and even failed: cyberattacks are on the rise, the efficacy of deterrence is questionable, and offensive approaches cannot stem the tide of small-scale attacks that threaten the world’s modern, digital foundations. Massive exploits—such as the recent hacks of SolarWinds’ network management software and Microsoft Exchange Server’s email software—are less a failure of U.S. cyberdefenses than a symptom of how the targeted systems were conceived and constructed in the first place. The goal should be not to stop all cyber-intrusions but to build systems that are able to withstand incoming attacks. This is not a new lesson. When cannons and gunpowder debuted in Europe in the fourteenth and fifteenth centuries, cities struggled to survive the onslaught of the new firepower. So states adapted their fortifications—dug ditches, built bastions, organized cavaliers, constructed extensive polygonal edifices—all with the idea of creating cities that could survive a siege, not stop the cannon fire from ever occurring. The best fortifications were designed to enable active defense, wearing the attackers down until a counterattack could defeat the forces remaining outside the city.

The fortification analogy invites an alternative cyberstrategy in which the focus is on the system itself—whether that’s a smart weapon, an electric grid, or the mind of an American voter. How does one build systems that can continue to operate in a world of degraded trust? Here, network theory—the study of how networks succeed, fail, and survive—offers guidance. Studies on network robustness find that the strongest networks are those with a high density of small nodes and multiple pathways between nodes. Highly resilient networks can withstand the removal of multiple nodes and linkages without decomposing, whereas less resilient, centralized networks, with few pathways and sparser nodes, have a much lower critical threshold for degradation and failure. If economies, societies, governments, and the international system are going to survive serious erosions of trust, they will need more bonds and links, fewer dependencies on central nodes, and new ways to reconstitute network components even as they are under attack. Together, these qualities will lead to generalized trust in the integrity of the systems. How can states build such networks?

First, at the technical level, networks and data structures that undergird the economy, critical infrastructure, and military power must prioritize resilience. This requires decentralized and dense networks, hybrid cloud structures, redundant applications, and backup processes. It implies planning and training for network failure so that individuals can adapt and continue to provide services even in the midst of an offensive cyber-campaign. It means relying on physical backups for the most important data (such as votes) and manual options for operating systems when digital capabilities are unavailable. For some highly sensitive systems (for instance, nuclear command and control), it may be that analog options, even when less efficient, produce remarkable resilience. Users need to trust that digital capabilities and networks have been designed to gracefully degrade, as opposed to catastrophically fail: the distinction between binary trust (that is, trusting the system will work perfectly or not trusting the system at all) and a continuum of trust (trusting the system to function at some percentage between zero and 100 percent) should drive the design of digital capabilities and networks. These design choices will not only increase users’ trust but also decrease the incentives for criminal and state-based actors to launch cyberattacks.

Making critical infrastructure and military power more resilient to cyberattacks would have positive effects on international stability. More resilient infrastructure and populations are less susceptible to systemic and long-lasting effects from cyberattacks because they can bounce back quickly. This resilience, in turn, decreases the incentives for states to preemptively strike an adversary online, since they would question the efficacy of their cyberattacks and their ability to coerce the target population. Faced with a difficult, costly, and potentially ineffective attack, aggressors are less likely to see the benefits of chancing the cyberattack in the first place. Furthermore, states that focus on building resilience and perseverance in their digitally enabled military forces are less likely to double down on first-strike or offensive operations, such as long-range missile strikes or campaigns of preemption. The security dilemma—when states that would otherwise not go to war with each other find themselves in conflict because they are uncertain about each other’s intentions—suggests that when states focus more on defense than offense, they are less likely to spiral into conflicts caused by distrust and uncertainty.

HUMAN RESOURCES

Solving the technical side, however, is only part of the solution. The most important trust relationships that cyberspace threatens are society’s human networks—that is, the bonds and links that people have as individuals, neighbors, and citizens so that they can work together to solve problems. Solutions for making these human networks more durable are even more complicated and difficult than any technical fixes. Cyber-enabled information operations target the links that build trust between people and communities. They undermine these broader connections by creating incentives to form clustered networks of particularized trust—for example, social media platforms that organize groups of like-minded individuals or disinformation campaigns that promote in-group and out-group divisions. Algorithms and clickbait designed to promote outrage only galvanize these divisions and decrease trust of those outside the group.

Governments can try to regulate these forces on social media, but those virtual enclaves reflect actual divisions within society. And there’s a feedback loop: the distrust that is building online leaks out into the real world, separating people further into groups of “us” and “them.” Combating this requires education and civic engagement—the bowling leagues that Putnam said were necessary to rebuild Americans’ social capital (Putnam’s book *Bowling Alone*, coincidentally, came out in 2000, just as the Internet was beginning to take off). After two years of a global pandemic and a further splintering of Americans into virtual enclaves, it is time to reenergize physical communities, time for neighborhoods, school districts, and towns to come together to rebuild the links and bonds that were severed to save lives during the pandemic. The fact is that these divisions were festering in American communities even before the pandemic or the Internet accelerated their consolidation and amplified their power. The solution, therefore, the way to do this kind of rebuilding, will not come from social media, the CEOs of those platforms, or digital tools. Instead, it will take courageous local leaders who can rebuild trust from the ground up, finding ways to bring together communities that have been driven apart. It will take more frequent disconnecting from the Internet, and from the synthetic groups of particularized trust that were formed there, in order to reconnect in person. Civic education could help by reminding communities of their commonalities and shared goals and by creating critical thinkers who can work for change within democratic institutions.

BOWLING TOGETHER

There’s a saying that cyber-operations lead to death by a thousand cuts, but perhaps a better analogy is termites, hidden in the recesses of foundations, that gradually eat away at the very structures designed to support people’s lives. The previous strategic focus on one-off, large-scale cyber-operations led to bigger and better cyber-capabilities, but it never addressed the fragility within the foundations and networks themselves.

Will cyberattacks ever cause the kind of serious physical effects that were feared over the last two decades? Will a strategy focused more on trust and resilience leave states uniquely vulnerable to this? It is of course impossible to say that no cyberattack will ever produce large-scale physical effects similar to those that resulted from the bombing of Pearl Harbor. But it is unlikely—because the nature of cyberspace, its virtual, transient, and ever-changing character, makes it difficult for attacks on it to create lasting physical effects. Strategies that focus on trust and resilience by investing in networks and relationships make these kinds of attacks yet more difficult. Therefore, focusing on building networks that can survive incessant, smaller attacks has a fortuitous byproduct: additional resilience against one-off, large-scale attacks. But this isn’t easy, and there is a significant tradeoff in both efficiency and cost for strategies that focus on resilience, redundancy, and perseverance over convenience or deterring and defeating cyberthreats. And the initial cost of these measures to foster trust falls disproportionately on democracies, which must cultivate generalized trust, as opposed to the particularized trust that autocracies rely on for power. This can seem like a tough pill to swallow, especially as China and the United States appear to be racing toward an increasingly competitive relationship.

Despite the difficulties and the cost, democracies and modern economies (such as the United States) must prioritize building trust in the systems that make societies run—whether that’s the electric grid, banks, schools, voting machines, or the media. That means creating backup plans and fail-safes, making strategic decisions about what should be online or digital and what needs to stay analog or physical, and building networks—both online and in society—that can survive even when one node is attacked. If a stolen password can still take out an oil pipeline or a fake social media account can continue to sway the political opinions of thousands of voters, then cyberattacks will remain too lucrative for autocracies and criminal actors to resist. Failing to build in more resilience—both technical and human—will mean that the cycle of cyberattacks and the distrust they give rise to will continue to threaten the foundations of democratic society.

Source URL: https://www.foreignaffairs.com/articles/world/2021-12-14/world-without-trust