DAKOTA DIGITAL REVIEW

Cloudification of Skills Training & "Dirty Jobs"
Mark P. Mills

North Dakota's UAS Ecosystem
Sen. Kevin Cramer

Artificial Intelligence is Transforming Our World —Are We Ready?
Nikola L. Datzov

Trouble in the Metaverse —Whatever That Is
Jeremy Straub

Whangdepootenawah!?
Patrick J. McCloskey

FALL-WINTER 2022-23

DAKOTA DIGITAL ACADEMY
NORTH DAKOTA UNIVERSITY SYSTEM

DAKOTA DIGITAL DISCUSSIONS FALL 2022

DAKOTA DIGITAL DISCUSSIONS is a webinar series offered by Dakota Digital Academy and Dakota Digital Review for the North Dakota University System. The talks focus on the ongoing impact of digitization, artificial intelligence and autonomous systems on the economy, culture, politics, military, law, arts and humanities, and the human psyche.

SEPTEMBER 21 AT 12 NOON

NIKOLA DATZOV, Assistant Professor of Law, University of North Dakota. Prof. Datzov's talk will be based on his article in the fall issue of Dakota Digital Review: *"Artificial Intelligence is Transforming Our World: Are We Ready?"*

OCTOBER 13 AT 12 NOON

ZAHID ANWAR, PHD, Associate Professor of Cybersecurity in the Department of Computer Science and scholar at the Challey Institute for Global Innovation and Growth at North Dakota State University. Prof. Anwar's talk will be based on his article in the fall issue of Dakota Digital Review: *"Overlooked Security Challenges in Electric Vehicle Charging Infrastructure."*

NOVEMBER 2, 4:00-5:30 P.M.

MARK MILLS, senior fellow at the Manhattan Institute, co-sponsored with the Challey Institute's Menard Family Distinguished Speaker Series. The talk, entitled "The Next Boom: It's Still Coming," is based on his recent book, *The Cloud Revolution,* and on his article in the fall issue of Dakota Digital Review: *"Cloudification of Skills Training & 'Dirty Jobs.'"* This talk will be presented both as a webinar and in person at the Louise S. Barry Auditorium at the Challey Institute for Global Innovation and Growth, Fargo, ND.

DECEMBER 6 AT 12 NOON

MARCUS FRIES, PHD, Associate Professor and Chair of the Department of Mathematics and Computer Science at Dickinson State University. Prof. Fries's talk will be based on his article in the fall issue of Dakota Digital Review: *"The Unencrypted History of Cryptography."*

To join the DAKOTA DIGITAL DISCUSSIONS, please visit Dakota Digital Academy's website at dda.ndus.edu

For more information, please contact patrick.mccloskey.1@ndus.edu

---

DAKOTA DIGITAL ACADEMY serves the 11 colleges and universities in the North Dakota University System, as well as the state's five affiliated tribal colleges and a private university:

BISMARCK STATE COLLEGE
DAKOTA COLLEGE AT BOTTINEAU
DICKINSON STATE UNIVERSITY
LAKE REGION STATE COLLEGE
MAYVILLE STATE UNIVERSITY
MINOT STATE UNIVERSITY
NORTH DAKOTA STATE COLLEGE OF SCIENCE
NORTH DAKOTA STATE UNIVERSITY
UNIVERSITY OF NORTH DAKOTA
VALLEY CITY STATE COLLEGE
WILLISTON STATE COLLEGE
CANKDESKA CIKANA COMMUNITY COLLEGE
NUETA HIDATSA SAHNISH COLLEGE
SITTING BULL COLLEGE
TURTLE MOUNTAIN COMMUNITY COLLEGE
UNITED TRIBES TECHNICAL COLLEGE
UNIVERSITY OF MARY

DAKOTA DIGITAL REVIEW

dda.ndus.edu/ddreview/

CONTENTS ▪ FALL/WINTER 2022

Cover: Scene from Steven Spielberg's "Ready Player One" (2018) in which the main character (played by Tye Sheridan) uses VR equipment to connect to the Oasis, a fictional concept similar to what some experts predict the metaverse could be like.

Introduction to the DAKOTA DIGITAL ACADEMY

KENDALL E. NYGARD, PHD

Director, Dakota Digital Academy,
North Dakota University System
Emeritus Professor, Department of Computer Science,
North Dakota State University
Contact: kendall.nygard@ndus.edu
Website: dda.ndus.edu

After our founding in the fall of 2020, the Dakota Digital Academy continues to gain traction with faculty and administrators across the North Dakota University System (NDUS). Thanks to the vision of Chancellor Mark Hagerott, there is much Dakota Digital Academy activity around designing and developing courses in the digital arena, configuring certificates and programs, creating partnerships and planning events. We are actively developing and promoting cooperative programs that can be earned in accelerated timeframes. DDA is focused on the need for relevant training and education to serve learners and employers.

We are ambitious and on track to accomplish a great deal in our state. We are committed to fostering access, opportunity, enfranchisement, inclusion and diversity. We believe in collaboration. Among Dakota Digital Academy's challenges is establishing synergy among the diverse NDUS institutions. With two research universities, four regional universities and five colleges, there are considerable differences in orientations, types of expertise and capacities. As well, the Dakota Digital Academy has entered into agreements with the state's five tribal colleges and one private university, which adds significantly to the system's scope. At the Dakota Digital Academy, we view the differences among institutions as sources of opportunities and strengths to celebrate.

The recent pandemic is one of the most life- and work-altering events in our history. This coronavirus forced a large-scale normalization of remote work and school, including mandating how the Dakota Digital Academy as an organization functioned. Going forward, if most tasks can be accomplished remotely and most production processes are done by robots, will gender inequality and racism diminish?

North Dakota is a very rural state. The Dakota Digital Academy is committed to location-agnostic operations. As broadband becomes more available and residents adjust to technologies—such as tools for remote collaboration, video conferencing and virtual reality—people may feel that if everyone in their organization is remote, then nobody feels remote.

Dakota Digital Academy's mission is very opportune in our state. If the future is basically digital, what happens to the people left behind? We see a pressing need for training and education in many areas of computing and cyber sciences, including coding, information technology, cybersecurity and artificial intelligence. Important application areas, such as energy and agriculture, have increasingly become digital enterprises. In terms of programs, the Dakota Digital Academy is actively working beyond cybersecurity and software development into these application areas.

The need for upskilling and retraining is also very real. Dakota Digital Academy is committed to helping meet those needs. ▣

DAKOTA DIGITAL REVIEW
Cloudification of Skills Training & "Dirty Jobs"
Mark P. Mills
North Dakota's UAS Ecosystem
Sen. Kevin Cramer
Artificial Intelligence is Transforming Our World —Are We Ready?
Nikola L. Datzov
Trouble in the Metaverse —Whatever That Is
Jeremy Straub
Whangdepootenawah!?
Patrick J. McCloskey
FALL-WINTER 2022-23
DAKOTA DIGITAL ACADEMY
NORTH DAKOTA UNIVERSITY SYSTEM

Introduction to DAKOTA DIGITAL REVIEW

PATRICK J. MCCLOSKEY

Editor, Dakota Digital Review
Director, Social & Ethical Implications of Cyber Sciences
Dakota Digital Academy
North Dakota University System
patrick.mccloskey.1@ndus.edu
Website: dda.ndus.edu/ddreview

The cartoonist Walt Kelly said it best, "We are confronted with insurmountable opportunities." What sorcerer or ancient magician could have imagined what we take for granted today: video conferencing across continents, texting at 30,000 feet on a jet liner, data mining, robotic surgery. And this is just the beginning. Digital wonders we can't envision yet will delight us and perform seeming miracles for the good of humanity.

As cyber technologies become increasingly ubiquitous, however, their penetration into our personal, family, professional and social lives is accelerating, and their influence is growing. In response, DDA will offer courses in the profound social, ethical, legal and policy implications of the cyber sciences.

To amplify DDA's systemwide approach across 11 colleges and universities, and to engage and educate the general public, DDA now presents Dakota Digital Review, which is being published both in print and online.

Dakota Digital Review will cover the cyber sciences, as well as related legal, political, regulatory, social and ethical issues, and digitization's impact on the humanities and the arts.

In addition to creating opportunities, digital technologies pose serious challenges: cybersecurity hacks by enemy nation states disrupting corporations, government agencies and even, December 2020, one of the world's largest cybersecurity firms; the massive transfer of power and wealth from small and analogue businesses to Big Tech companies as result of lockdown responses to COVID-19; blatant censorship by Big Tech that threatens free speech and the foundations of democracy; disinformation campaigns and election integrity; privacy and surveillance concerns; artificial intelligence (AI), automation and job loss; rural broadband, especially when students must take classes from home.

Dakota Digital Review is written and edited for the general educated reader. It is vitally important that residents throughout the region—whether working in government or business, or who are retired—become fluent and engaged in cyber sciences and their ramifications.

Articles are written mostly by faculty and students but not to promote their universities. Instead, higher education's intellectual resources are being mobilized statewide to better serve both within and beyond the academy.

Dakota Digital Review elevates discussions and debates about digitization, facilitating better preparation of government and business, parents, students and voters to make crucial decisions about our collective future and about our individual and family lives.

A note of appreciation is due to Jerry Anderson who does the photography, graphic design and layout for Dakota Digital Review, as well as to Tom Marple for illustrations. The same is due to Kay Cox who designs and masters our website (URLs above), where access to our courses and this magazine is available. ▣

Cloudification of Skills Training & “Dirty Jobs”

MARK P. MILLS, Senior Fellow, Manhattan Institute

Competition for the increasing limited supply of those with skills is driving up wages, which is an obvious benefit for the employee, but is also inflationary for the employer’s product or service. And it doesn’t increase the supply until more people are attracted to those trades, and then not until they’re trained. Thus begins a boom for skills training.

While popular media focuses on “higher ed” issues, the long-ignored challenges are in expanding the availability of schools that teach skills associated building, maintaining and operating the essential physical infrastructures of our society, from highways to hospitals, and from semiconductor fabs (fabrication plants) to the shale fields. These are all the kinds of skilled jobs that were labeled “essential” in the months of the Great Lockdowns. They’re also often the “dirty jobs,” as TV’s Mike Rowe, the champion of such work, labeled them. They’re the kind of jobs that require people to show up, to be hands-on.

As everyone knows, in the normal course of history’s progress, the nature of work is always changing. Many specific kinds of skills that were essential in the past are no longer needed. Different types of work emerge as the structures of industry and service change with society. Some 60 percent of the jobs that existed as recently as 1960 no longer exist as forms of employment. There is nothing new about the idea that this shifting landscape requires workers to upskill or reskill, to earn new knowledge and often formal certifications from schools of “continuing education.” What *is* new is that, for the first time, the source of much of the current workplace disruption, the Cloud, is simultaneously enabling better means for all the reskilling it necessitates.

"Tastes Like Cotton Candy," oil on canvas, Britta Anderson, 2022,

Courtesy of The Capital Gallery, Bismarck, ND

In the face of an economic slowdown, or even the possibility of a recession, America still has a shortage of skilled labor in every domain from home construction to the great shale oil fields, as in the Bakken.

The domain of skills, and learning them, divides neatly into two camps. There are skills that are essentially informational, and those that are, literally, hands-on. The former involves understanding ideas—specific regulations, permissions, safety standards, associated with, say, driving an excavator at a construction site. Such knowledge can be acquired without setting foot in an excavator. But learning how to operate the excavator itself requires hands-on training.

Much has been made over the differences between learning in these two domains in terms of how much computers can help. Some three decades ago, leading computer scientists observed what is now often called "Moravec's Paradox" (named after Hans Moravec): the irony that it's easier to teach a computer to play chess than, say, fold laundry. It's ostensibly a paradox because the former is referred to as a "high-level" task, whereas the latter is "low-level." This sort of hierarchical categorization, however, fails to recognize that physical tasks entail an exquisitely complex integration of—high-level—human sensory capabilities, neuro-motor skills and reasoning. To put somewhat facetiously: It's the difference between teaching children to spell "excavator" and teaching them to operate one.

Cloud Democratization of AI

We'll come back to the physical skills. The revolution in learning non-physical skills is not that they can be taught online or remotely. That's been possible for quite a while, whether through TV, VCR, audio tapes or even radio. It is, of course, meaningful that remote training can now scale up rapidly, along with the Cloud's infrastructure. But the unique distinction of future developments will be the Cloud's democratization of AI, which will enact a different kind of disruption to teaching informational skills.

Looking at the changes in information since 1970, Massachusetts Institute of Technology (MIT) economists David Autor and Anna Salomons documented the shift in the structure of employment and, specifically, the hollowing out of highly paid "middle-skilled" jobs that typically don't require a college degree.[i] The two general categories of such middle-skilled jobs that faced the greatest declines were physical operations and office administration. Physical operations were hollowed out mainly because of machine automation and industrial outsourcing. The decline in administrative employment was caused by the kinds of software that emerged in the late 20th century—word processing, filing, mailing, drawing, printing and spreadsheets—shifting clerical tasks away from middle-skilled employees to the desktops of professionals. AI will do the inverse with many of the "higher-order" skills currently in the domains of the professional class.

Up until now, analytical software tools have typically focused on the collection, storage and presentation of data, and have required fairly sophisticated training and education to operate. AI pattern-recognition and advice-giving—including using real-time simulations and "virtual twin" models—now routinely assist the professional manager. But as those AI tools become more intuitive, that advice can be delivered directly to the "middle-skilled," non-college-educated employee too.

Managers and engineers are deluged with data about myriad factors relating to operational efficiency (and safety): sources, quantities, changes in location or composition of inputs, suppliers, and market dynamics. Recognizing patterns in all the information is what constitutes most daily operational decisions. But it's in precisely these kinds of areas of complexity where AI can advise and even automate, looking for the "signal in the noise." Such information automation pushes the ability for such decision-making out to the front lines of a factory floor or hotel front desk in the form of "virtual" assistants that "upskill" the capabilities of non-management employees.

Thus, a key feature of AI is found not in those "intelligent machines" necessarily making autonomous decisions, the feature that causes so much anxiety among prognosticators, but instead in its ability to provide informed advice with a "natural language interface" that requires neither programming skills nor special expertise. Such AI-enabled operational guidance, "intelligent digital assistants," can operate in real-time on those front lines, whether it involves machinery or supply chain decisions that entail considering hidden complexities formerly the purview of the management class. And that AI-driven guidance and advice will be delivered, increasingly, not only in natural language but also in augmented (AR) and virtual reality (VR) interfaces.

Software in the pre-AI era led to tools such as Computer Aided Design (CAD), which mainly helped engineers in their work and eliminated the need for draftsmen. In the AI-enabled world, engineering design and even some professional aspects of manufacturing will shift to the employees doing the work rather than those managing the work. The same dynamic is coming to the IT world itself. As with manufacturing, Computer Aided Software Engineering tools have been around for many decades. But now we have AI tools that allow "programming without code." In other words, coders are working to put other coders out of a job by creating Cloud-based tools that a nonexpert can use to create software.[ii]

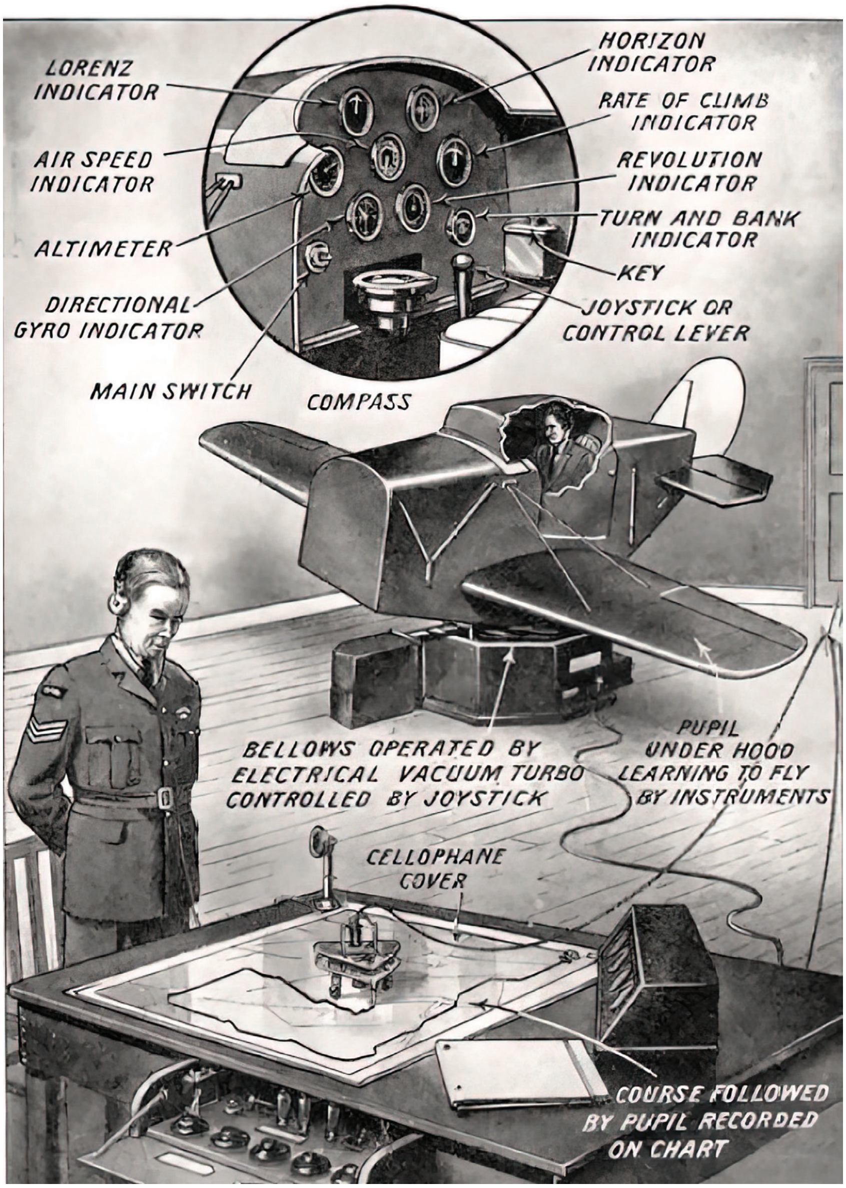
Big tech companies such as Oracle, Salesforce, Google and Microsoft, as well as numerous startups, are in a race to produce ever-simpler "no-code software" tools, with which customers can use natural language, intuitive graphics and interfaces to write code without knowing a jot of it. This doesn't signal the end of coding as a profession any more than automation signaled the end of farming or construction jobs. But it does signal that coders at or above the college level will continue to be a small fraction of the share of people employed overall. Today, roughly as many software engineers exist as do people employed on farms or construction sites. Odds are good those will all remain niche occupations over the coming decade. More importantly, the democratization of software-creation will accelerate the nonexpert use of AI-enhanced tools in every profession.

Farmers, as it happens, are ahead of the curve in this trend (as they were with industrialization). Not only is farm equipment now often autonomously navigated, but decisions farmers make about what and when to plant, irrigate and fertilize are all delivered on-site with real-time data *and* analytic advice from Cloud-centric, AI-driven software. Another implicit bellwether of this trend was when UPS, in late 2020, offered early buyouts to many management employees while simultaneously hiring 100,000 workers for the holidays.[iii] The net effect of all this real-time "upskilling" of the nonexperts will "hollow out" many jobs formerly reserved for those classified as professionals. More efficient. More production. And more disruption.

Driving Excavators & Exoskeletons

We owe to a high-school dropout the idea of using a simulator to help learn the skills of operating complex or dangerous machines. Edwin Link sold his first aircraft flight simulator in 1929. It was the first example of useful "virtual" reality, an idea Link concocted because of his love of flying—he purchased Cessna's first airplane—and his understanding the risks of learning how to fly.[iv] Accidents and fatalities were notoriously high in those early days of commercial aviation.

Link's eponymous machine would prove critical for training thousands of pilots in World War II. A complete aircraft cockpit (i.e., no wings or fuselage,


LORENZ INDICATOR
AIR SPEED INDICATOR
ALTIMETER
DIRECTIONAL GYRO INDICATOR
MAIN SWITCH
COMPASS
HORIZON INDICATOR
RATE OF CLIMB INDICATOR
REVOLUTION INDICATOR
TURN AND BANK INDICATOR
KEY
JOYSTICK OR CONTROL LEVER
BELLOWS OPERATED BY ELECTRICAL VACUUM TURBO CONTROLLED BY JOYSTICK
PUPIL UNDER HOOD LEARNING TO FLY BY INSTRUMENTS
CELLOPHANE COVER
COURSE FOLLOWED BY PUPIL RECORDED ON CHART

During World War II, Edwin Link's AN-T-18 Basic Instrument Trainer was standard equipment at every air training school in the United States and Allied nations.

etc.) with instruments and controls that responded to the pilot by moving on hydraulics created the illusion of flying and thus allowed development of the necessary reflexes. (Early on it was far from as realistic as today's simulators, but it was good enough to see a dramatic decrease in accidents from novice pilots.) His company still exists today: Via a number of different acquisitions, it is now part of defense contractor L-3 Technologies. And today's technology, while profoundly more sophisticated, differs little in concept and plays a central role in both training pilots and designing new aircraft.

After Link, the next pivot in the path to a broader application of VR simulators came in 1966 from Tom Furness, an electrical engineer and Air Force officer. Furness invented the idea of a helmet-mounted heads-up display as a solution to the rising complexity of cockpit instruments. That idea earned him the title of "godfather of virtual reality." Furness, like Link, went on to create a company, indeed, dozens of them. Most recently he founded the non-profit Virtual World Society to help advance VR as a learning tool for families.[v] Today, heads-up displays are standard flight equipment, and the U.S. military trains its fleet

The first excavator simulator didn't arrive until just after Y2k. Other heavy equipment simulators then followed quickly with such training now as firmly established as flight simulation.

A man wearing a virtual reality (VR) headset—also called "VR goggles"—that provides an immersive 3D experience in a simulated environment. VR headsets must be connected to a computer or a smartphone. As well, there are Augmented Reality (AV) headsets, also known as smart glasses, and combo AR/VR goggles. Some AV glasses are capable of displaying holographic images.

of drone pilots on machines built by the L-3 Link Simulation & Training division, directly descended from Edwin Link's innovation.

But until recently, only a sliver of the myriad tasks involved in learning a skill have been amenable to simulation, whether using a wood lathe, welding, plumbing or driving an excavator. In fact, the first excavator simulator didn't arrive until just after Y2k.[vi] Other heavy equipment simulators then followed quickly with such training now as firmly established as flight simulation.[vii] The market for skills simulation and training is, self-evidently, far wider than that for expensive heavy equipment and high-cost aircraft.

The demand for skills is poised to soar not only because of the new skills that will be needed for the new kinds of machines, from warehouse robots and delivery drones, to cobots (collaborative robots) in hospitals, but also because of the so-called "silver tsunami." The economies of all the developed nations face the unavoidable demographics of the aging of the skilled workforce. The cohort of employees performing skilled tasks skews heavily to those nearer retirement age. This means that, once this group retires, the existing "skills gap" will grow and the demand for simulators to train employees more effectively, quickly and inexpensively will grow as well.

The continual advances in virtual reality have, so far, come at a cost. Link sold his trainers to the Army Air Corps in the 1930s for $65,000 (in today's inflation-adjusted dollars). Flight simulators now cost from $1 million without motion control to as much as $10 million with full dynamic motion. That may be tolerable for training people how to fly aircraft that cost from $10 to $100 million. But simulators with physical and tactile feedback will need to become cheaper for them to break into other domains—excavators, yes, but also all other kinds of machines, from expensive exoskeletons to remotely operated delivery drones to many classes of semi-autonomous cobots. Lower costs at higher performance are precisely the metrics that the AI, microprocessor and materials revolutions are bringing to simulators.

AR/VR: Over-Promised & Underestimated

In the early days of VR, there was rampant over-promising of what could be achieved, a common phenomenon with new technologies. Facebook famously spent $2 billion to buy the VR company Oculus in 2014, hoping that VR would rapidly enter common usage. It didn't happen. But now, finally, the three enabling technologies underlying useful VR have reached the necessary collective tipping point.

Realism in VR still begins with the visual. The researchers chasing ever-greater screen resolution, for both large room-scale and tiny eyeglass-size displays, have achieved near life-like pixel densities, with more coming at lower cost. Image generation in real-time gets computationally harder as the pixel density rises. And any image time lag in VR systems has been documented to generate not just a sense of disbelief in the scene, but also fatigue, disorientation and even nausea. That's being conquered now with superfast image rendering from hyper-performance GPUs. Redolent of how the progenitor of the first cellphone said that Dick Tracy comics inspired that invention, we find Taylor Scott, inspired by the iconic scene of Princess Leia in a holographic display in the 1977 Star Wars movie, unveiling in early 2021 a (prototype) smartphone display that produces a 3D holographic image without special goggles.[viii]

The newest low-cost, high-performance AI engines also play a key role in moving VR systems to the next level. Facebook, not deterred from earlier false steps, has developed an AI-driven system that can dynamically track the user's eyesight to integrate what's seen with what's being heard. This allows the system to replicate our brain's ability to focus selectively on "hearing" what we are seeing, blocking out the ambient sound of a noisy environment.[ix] Conquering that particular feature of VR has been called the "cocktail party challenge." Solving it will, separately, revolutionize hearing aids. AI engines can also use motion detection combined with cameras to analyze emotional state, puzzlement or attention level. These emotion-sensing technologies (EST) are being added to simulators, but they're also showing up as driver-assistance tech in automobiles (and other machines for which attention matters greatly).

In order for AR/VR to have the feel of reality, the human–machine interface also has to become more natural in its reception of our "input" commands. In an ideal interface, the machine (or image, or algorithm) should both respond to intentional instructions and intuit our intent. To accomplish the latter, engineers have developed interfaces that "see" our motions and actions to predict an intent. These are either called touch-free systems or intuitive gesture control systems. There are now dozens of such devices—from big companies such as Google and Microsoft, as well as startups. (As has always happened—and is the intended outcome for many entrepreneurs and investors—many of the latter get acquired by the former.)

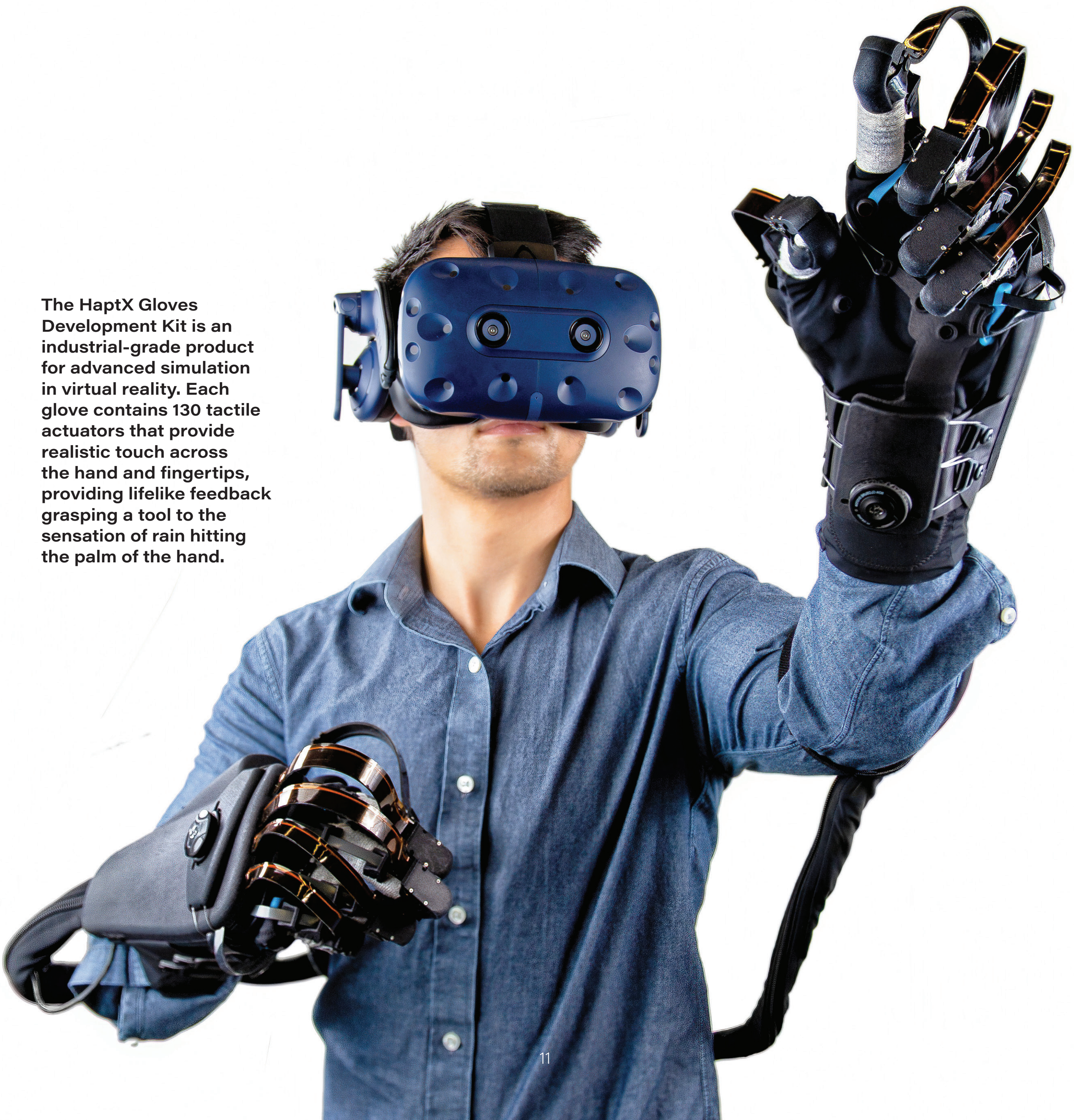
The concept is not new. Canada's Gesturetek, for example, provided hands-free video-based input control starting some 30 years ago, used in museums, stores and bars. But it is only in the last five or six years that simple gesture control has matured through the arrival of advanced, tiny and cheap sensors and logic chips. Across the entire applications range, from games and appliances to cars and military machines, the market for gesture-intuitive interface devices is already measured in the tens of billions of dollars.[x]

Some of those control devices are based entirely on cameras or acoustic sensors (microphones) that are already native in smartphones and cars, combined with AI and machine learning to watch, analyze and intuit intent. Some devices also take advantage of the exquisite sensitivity of silicon MEMS (micro-electromechanical systems) microphones that enable detection of both breathing and heartbeat; aside from health monitoring implications, that data can help analyze anxiety or attention. Others, such as Google's Motion Sense, use tiny, active radar chips to track gestures. And some input devices fuse a combination of or all of the aforementioned sensing modalities.

While we're quite a way away from a future (despite interesting research into the possibility) in which we can directly read the challenging and "noisy" signals radiating from our brain's neurons, at least one company has developed a clever wristband that focuses instead on measuring and interpreting neural activity in your wrist—the messages the brain sends to direct the hands. The latter, developed by the aptly named CTRL-Labs (bought by Facebook in 2019), enables computers to see, interpret and realistically simulate profoundly complex actions, such as playing a piano.

Age of "Vibrotacticle Haptics"

But one of the critical elements still missing from nearly every VR system is physical feedback, particularly tactile feedback. (Link's flight simulators use electro-hydraulics to simulate bulk motion, as do Disneyland rides.) The idea of a tangible user interface, or a tangible internet, where one can feel images, finds its origins at the MIT Media Lab in 1997.[xi] It is the last remaining feature needed to bring VR technology one step closer to true realism for many tasks, and what



The HaptX Gloves Development Kit is an industrial-grade product for advanced simulation in virtual reality. Each glove contains 130 tactile actuators that provide realistic touch across the hand and fingertips, providing lifelike feedback grasping a tool to the sensation of rain hitting the palm of the hand.

[T]echnologies now exists to enable, in the 2020s, hyper-realistic virtual simulators for skills training … [that will] also dramatically improve real-time, human-machine interfaces in heavy industries and service sectors.

the researchers 20 years ago at Xerox PARC termed the "age of responsive media."[xii]

In order to virtually sense touch, one needs actuators that replicate—ideally, biomimic—what nerve and muscle cells do. That old dream is realizable now because of the quiet revolution in materials sciences, and the complementary revolution in precision fabrication machines that can make devices out of those novel materials. With electrically reactive polymers and flexible ceramics, the age of "vibrotacticle haptics" is emerging, taking the technology a leap past the familiar vibrating smartphone that has been around for more than a decade. Gloves made from active polymers can serve as both sensor (telling the simulator what your hand is doing) and actuator (providing the sensation of touching a virtual object). And for actions that involve bigger forces, say turning a valve, gloves can have a powered mini-exoskeleton.

As for the more subtle sensing associated with, say, textures, engineers have found ways to program a display's surface to trick fingers into "feeling" virtual features. By subtle control of electrical forces on the surface of a screen, nerves in fingers can be told to 'feel' a bump or feature. Aligning that tactile sense with an image gives the illusion of feeling the texture of the image. This is done by building microscopic conductive layers into displays using the same tools and materials already employed to build the displays.

Such haptics are first targeting making automotive displays safer by allowing the driver to use them by feel. The same technology leads to not only a more reliable control panel or dashboard of switches (since it's no longer mechanical but virtual), but also a more customizable one that can be easily upgraded.[xiii] As the technology of hard displays migrates into the technology of flexible, conformal displays, the haptic surface can be wrapped around the shape and contours of objects including, eventually, hands.[xiv] Such "artificial skin" is now in a prototype stage analogous to touch screens for phones were *circa* late 1990s. It wasn't long after that (2007) that the market-changing iPhone was launched. The 2020s will see tactile-sensing "gloves" that are close to skin-like.

The suite of technologies now exists to enable, in the 2020s, hyper-realistic virtual simulators for skills training for many applications beyond big machines, and also to see such capabilities available remotely. This will permit not only virtual but also online apprenticeship for many skilled trades. It will also dramatically improve real-time, human-machine interfaces in heavy industries and service sectors.

AR/VR: Distinctions & Forecast

Those who are sophisticated in these technologies will notice we have not distinguished, as the engineering community does, amongst the various types of virtual, augmented and mixed-reality systems. There are plenty of gradations between VR and AR, and there are many applications for both beyond skills training and education, including in nearly every aspect of commerce. VR attempts to create an entirely artificial simulation, in many cases a fully immersive environment wherein, for example, a technician or student can undertake a trail run on driving or repairing a machine's digital simulacrum. AR doesn't attempt to replicate reality but instead "augments" it by superimposing information and/or images onto reality. A repair technician (or physician) using AR glasses can see what's inside a machine before "lifting the hood," or a tourist looking at the Coliseum can see a rendering of what it might've looked like in Roman times, with historical information crawling like subtitles below the view.

For AR to break into common business use and everyday wear—to become as ubiquitous as, say, laptops—will require meeting consumers demands in performance, cost and fashion. It is a technological leap that is, in fact, comparable to going from desktops to laptops. But that prospect is now visible in the pre-commercial products emerging from various startups and from bigger tech companies such as Niantic, Facebook, Google and Apple.

Forecasters now see sales of AR/VR devices rising from 1 million units in 2020 to over 20 million by 2025. While businesses will account for 85 percent of those purchases, that's a similar percentage seen in the early adoption of desktop computers.[xv] What will subsequently follow is the embedding of AR capabilities into contact lenses. That idea is no longer fanciful but feasible, with notional prototypes using the emerging class of flexible, bio-compatible electronics.[xvi]

While education, healthcare and advertising are all big magnets for VR and AR—all are also the focus of enormous venture investments—the biggest single locus for VR and AR spending is found in entertainment.[xvii] Advances in the entertainment market will, just as they have throughout history, greatly benefit all others. And in particular, in our near future, the challenge of upskilling and training enough people to fill the looming gaps in the great skilled trades.

This article is an excerpt adapted from the book* The Cloud Revolution: How the Convergence of New Technologies Will Unleash the Next Economic Boom and a Roaring 2020s. *It is reprinted with permission of the author.

[i] Autor, David, and Anna Salomons. "New Frontiers: The Evolving Content and Geography of New Work in the 20th Century." NBER Economics of Artificial Intelligence, May 2019. https://stuff.mit.edu/people/Autor-Salomons-NewFrontiers.pdf

[ii] Caballar, Rina Diane. "Programming Without Code: The Rise of No-Code Software Development." IEEE Spectrum, March 11, 2020. https://spectrum.ieee.org/tech-talk/computing/software/programming-without-code-no-code-software-development.

[iii] Ziobro, Paul. "UPS Offering Buyouts to Management Workers." The Wall Street Journal, September 17, 2020. https://www.wsj.com/articles/ups-offering-buyouts-to-management-workers-11600378920.

[iv] McFadden, Christopher. "The World's First Commercially Built Flight Simulator: The Link Trainer Blue Box." Interesting Engineering, August 21, 2018. https://interestingengineering.com/the-worlds-first-commercially-built-flight-simulator-the-link-trainer-blue-box.

[v] Vanfossen, Lorelle. "Virtual Reality Pioneer: Tom Furness." Educators in VR, May 31, 2019. https://educatorsinvr.com/2019/05/31/virtual-reality-pioneer-tom-furness/.

[vi] "LX6 - Medium Fidelity Simulator Platform - Built for High Throughput Training." Immersive Technologies - Expect Results. Accessed April 15, 2021. https://www.immersivetechnologies.com/products/LX6-Medium-Fidelity-Training-Simulator-for-Surface-Mining.htm.

[vii] Vara, Jon. "Heavy Equipment Simulators." JLC Online, February 1, 2012. https://www.jlconline.com/business/employees/heavy-equipment-simulators_o.

[viii] Greig, Jonathan. "Using 'Star Wars' as Inspiration, Hologram Maker Imagines New Future for Smartphones." TechRepublic, March 16, 2021. https://www.techrepublic.com/article/using-star-wars-as-inspiration-hologram-maker-imagines-new-future-for-smartphones/

[ix] Dormehl, Luke. "Facebook Is Making AR Glasses That Augment Hearing." Digital Trends, November 1, 2020. https://www.digitaltrends.com/features/facebook-ar-glasses-deaf/.

[x] Brandessece Market Research, "Gesture Recognition Market," April 13, 2020. https://brandessenceresearch.com/PressReleases/gesture-recognition-market-is-expected-to-reach-usd-25551-99-million-by.

[xi] Ishii, Hiroshi. "Tangible Bits." *Proceedings of the 8th international conference on Intelligent user interfaces - IUI '03*, 2003. https://doi.org/10.1145/604045.604048.

[xii] Begole, James. "The Dawn Of The Age Of Responsive Media." Forbes, January 12, 2016. https://www.forbes.com/sites/valleyvoices/2016/01/12/the-dawn-of-the-age-of-responsive-media/#61d0eca8bce8.

[xiii] LoPresti, Phillip. "Surface Haptics: A Safer Way for Drivers to Operate Smooth-Surface Controls." Electronic Design, December 3, 2020. https://www.electronicdesign.com/markets/automotive/article/21145025/surface-haptics-a-safer-way-for-drivers-to-operate-smoothsurface-controls.

[xiv] Park, Sulbin, Byeong-Gwang Shin, Seongwan Jang, and Kyeongwoon Chung. "Three-Dimensional Self-Healable Touch Sensing Artificial Skin Device." *ACS Applied Materials & Interfaces 12*, no. 3 (2019): 3953–60. https://doi.org/10.1021/acsami.9b19272.

[xv] Needleman, Sarah E. and Jeff Horwitz, "Facebook, Apple and Niantic Bet People Are Ready for Augmented-Reality Glasses," Wall Street Journal, April 6, 2021. https://www.wsj.com/articles/facebook-apple-and-niantic-bet-people-are-ready-for-augmented-reality-glasses-11617713387.

[xvi] Kaplan, Jeremy. "Future of Vision: Augmented Reality Contact Lenses Are Here." Digital Trends, March 2, 2021. https://www.digitaltrends.com/features/augmented-reality-contact-lenses-vision/.

[xvii] "An Introduction to Immersive Technologies." Vista Equity Partners, August 10, 2020. https://www.vistaequitypartners.com/insights/an-introduction-to-immersive-technologies/.

Arrival of the first RQ-4 Global Hawk—an intelligence, surveillance and reconnaissance drone—at Grand Forks Air Force Base on May 26, 2011.
Credit: Tech. Sgt. Johnny Saldivar

North Dakota's UAS Ecosystem is Crucial to Keeping Up With Our Adversaries

THE HONORABLE KEVIN CRAMER
United States Senator for North Dakota

North Dakota has played a critical part in deterring our adversaries since the beginning of the Cold War. The Soviet Union always knew North-Dakota-based bombers, radars and intercontinental ballistic missiles were cutting edge and ready to deter Communist aggression. While many of these weapons still deter our peer adversaries today, times have changed and so have the threats. In response, North Dakota continues to play a leading role as we modernize our nuclear deterrence and develop Unmanned Aerial Systems (UAS) to face off against surging adversaries, such as China.

In October, I had the pleasure of speaking at the 15th annual UAS Summit & Expo in Grand Forks, where I highlighted this race for military technology and the rapidity at which this technology is growing, which I begrudgingly call "the speed of China." Unfortunately, China has passed us in the speed it takes to turn an idea (many times stolen) into a weapon, matching or exceeding our own.

A perfect example is the recent Chinese hypersonic weapons test. After being launched into orbit, a Chinese spacecraft, capable of carrying nuclear weapons, circumnavigated the globe at five times or more the speed of sound. Before reentry, according to news reports, the maneuverable glide vehicle fired one and perhaps two missiles while zooming high above the South China Sea—a remarkable engineering feat that surprised Pentagon scientists. Demonstrations like this are the reason why China should be considered no less than a peer adversary, and why we need to aggressively avoid being downgraded to a near-peer competitor.

So how do we respond to this kind of technological growth from our adversaries?

The short answer is the creation of an ecosystem that allows the technology to grow in as many directions as possible. The longer answer involves working with local, state and federal governments, as well as any and all regulatory branches, including the military, private sector, universities and anyone else who wants to participate. All these forces working in tandem enable technology to grow. This is by no means easy, but North Dakota has been making significant strides in developing a more encompassing UAS ecosystem.

North Dakota is blessed to have a population with expertise in operating UAS. Our Fargo Air National Guard started flying MQ-1 Predators and then MQ-9 Reapers in 2007, while Grand Forks Air Force Base started flying RQ-4 Global Hawks in 2011. The experience our airmen gained from operating critical missions around the world brought a sophisticated level of understanding of exactly how to effectively operate UAS—underscoring how valuable UAS technology is to the warfighter. This knowledge and experience will feed future growth.

With our Midwest work ethic and forward-thinking tendencies, the North Dakota Department of Commerce set up the Northern Plains UAS Test Site in 2013, as one of seven such sites nationwide designated by the Federal Aviation Administration (FAA). With state funding and the FAA's regulatory assistance, the test site has grown to include Beyond Visual Line of Sight (BVLOS) command links, which allow UAS to be flown far from their operators within identified sectors of the state. With FAA and Federal Communications Commission assistance, we hope to expand this statewide. North Dakota's accommodating environment, backed by federal agencies and the state's government, feeds growth.

With the local expertise of the military UAS base in Grand Forks, a positive vector for permissive regulations, available space adjacent to the base with access to the runway and detect-and-avoid radar capability, a partnership was formed with the U.S. Air Force, the County of Grand Forks and Grand Sky Development Company, LLC. This partnership created Grand Sky, the nation's first commercial UAS business and aviation park. Grand Sky now houses industry leaders, such as Northrop Grumman and General Atomics, which execute thousands of hours of training and testing for UAS in North Dakota airspace. These opportunities—from employment to runway access and airspace to BVLOS command links—all lead to expansion.

It's important to underscore the importance of having the UAS testing options North Dakota provides to companies and the military alike. For a technology or a capability to grow fast, it needs to be tested, possibly fail, and then be fixed and tested again. But options for UAS testing within the United States are very limited and often restricted to military ranges with busy schedules and other competing priorities. Additional delays often occur because companies work longer to lower risk before getting their limited chances to test. However, increasing opportunities for testing, as we're doing in North Dakota, means the technology can come off the drawing board quicker and advance to a proven system faster than our current process allows.

Institutions of higher education are also critical to development. In addition to the University of North Dakota's (UND) long history of teaching young men and women to fly, the university has been at the forefront of UAS growth for more than a decade. UND created the Research Institute for Autonomous Systems (RIAS), whose mission statement says it all: "Create new autonomous systems through multidisciplinary research and lead development of world-changing autonomous policies, with the goal of driving a vibrant, diverse and sustainable economy consistent with ethical and legal standards." RIAS's and UND's efforts have grown the talent base and incubated the innovation that feed growth.

And talent attracts talent, which is why North Dakota has been the destination for several distinguished visitors in the fields of science, technology and national defense. Recent visits by visionaries and leaders include NASA Administrator Jim Bridenstine; Chief of Space Operations, U.S. Space Force, General Jay Raymond; Director of the Space Development Agency Derek Tournear, PhD; Secretary of the Air Force Frank Kendall; Air Force Chief of Staff General Charles Brown Jr.; and Chief of Naval Research Rear Admiral Lorin Selby, to name a few. These visits

Rear Adm. Lorin Selby, Chief of Naval Research, speaking at the 15th annual UAS Summit & Expo in Grand Forks, ND, in October 2021. Seated is Sen. Kevin Cramer whose talk highlighted the global race for military technology and the rapidity of technological growth, especially regarding China. Credit: Tech. Sgt. Johnny Saldivar

precipitate knowledge exchanges, which wouldn't happen without the draw of North Dakota's UAS ecosystem.

These are just a few examples of the reason why North Dakota has been recognized by the Mercatus Center at George Mason University as the number one state for UAS readiness. I could go on about the growth of space capabilities, both at our military bases and UND, and how this is directly tied into how we'll operate UAS. Or how the Range Hawk UAS capability, which is being developed at Grand Sky, will help test future hypersonic capabilities. Or how having permissive airspace for UAS is perfect for testing counter-UAS capabilities. Or how the Customs and Border Protection agency uses North Dakota's UAS ecosystem to train its UAS pilots. Or how none of this would be possible without the vision, support of and acceptance by the great people of North Dakota. Or Congressional leadership from the likes of U.S. Senator John Hoeven, which dates back to his days as governor, to establish North Dakota as a UAS hub positions North Dakota for success.

Ultimately, if we are going to keep up with China, the U.S. will have to build off North Dakota's success story. What we are doing will have a substantial effect on how we keep up with China and the rest of the world when it comes to UAS technology. And, North Dakota is setting the example for how other technologies need to grow. ▣

In addition to the University of North Dakota's long history of teaching young men and women to fly, the university has been at the forefront of UAS growth for more than a decade.

The Unenɔrypt3d Hiƨt8ry *of* Crypt□graphy

MARCUS FRIES, PHD
Associate Professor and Chair, Department of Mathematics & Computer Science
Dickinson State University

It is 58 B.C. and a Roman general sits atop a hill studying the opposing army, consisting of warriors from several Gallic tribes, in what is now a forested area on the eastern side of central France. He receives a message from Julius Caesar, his commander, and is quite certain no one else has read it.

Jenny logs into her bank account using her password. She is quite certain no one else can read her account balance or uncover her account number.

Kevin makes a purchase using his debit card and pin number. Again, he and his bank can be certain no one else is making this transaction.

What do these three situations have in common? All three involve some sort of secret sharing scheme. The study of secret sharing is known as cryptography. In this article, I will take you on a historical journey through this fascinating subject. In a future article, I will go over more of the science of cryptography.

Caesar Shift

One of the first recorded secret-sharing schemes is known as the Caesar Shift. The idea is to take a message and shift each letter in the text three places (or any number 1-25) forward or back in the alphabet: A→D, B→E, M→P, Z→C and then A→D again. The security is given by the key, which is how many places to shift the letters. Then anyone knowing the key can quickly read the message.

The Caesar Shift, while neat, is not very secure. In times of less literacy, it was secure, but in modern times it falls quite quickly to frequency analysis, using the fact that all letter As get encoded by the same letter (D) each time. This results in the relative frequencies of the letters and words staying the same: E is the most common letter—which would be H in this Caesar Shift. Similarly, "a," "an" and "the" are the most common words, which would become "d," "dq" and "wjh."

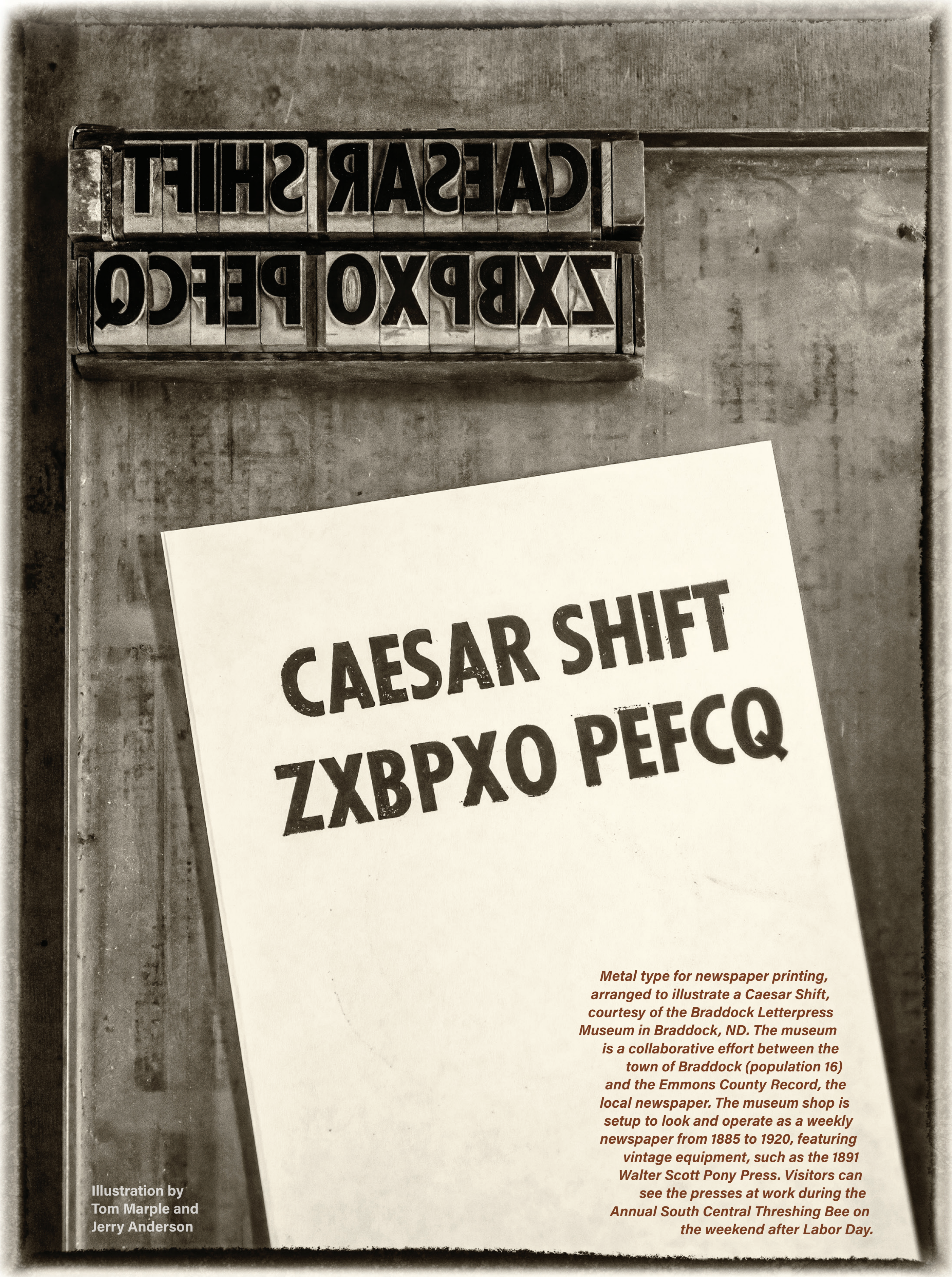


Illustration by Tom Marple and Jerry Anderson

Metal type for newspaper printing, arranged to illustrate a Caesar Shift, courtesy of the Braddock Letterpress Museum in Braddock, ND. The museum is a collaborative effort between the town of Braddock (population 16) and the Emmons County Record, the local newspaper. The museum shop is setup to look and operate as a weekly newspaper from 1885 to 1920, featuring vintage equipment, such as the 1891 Walter Scott Pony Press. Visitors can see the presses at work during the Annual South Central Threshing Bee on the weekend after Labor Day.

Illustration by Tom Marple and Jerry Anderson

Vigenère Cypher

The next step forward in cryptography was the Vigenère Cypher—chronicled first in 1553 by Giovan Battista Bellaso but then miscredited to another 16th century cryptographer Blaise de Vigenère—which uses a key word to shift the letters of the message. For example, if we pick the key word "dance," we would obtain a shift key of 4, 1, 14, 3, 5. Given the message "meet at noon," we would shift the first letter by 4, the second by 1, the third by 14, the fourth by 3, the fifth by 5, and then repeat: the sixth by 4 and so on. The advantage here is that two occurrences of E would be encoded differently, hence the frequency analysis would not be quite as effective.

As is the case with the Caesar Shift, there are known attacks on the Vigenère Cypher which are very effective at breaking it. They can be done by hand with some work.

With the Vigenère Cypher, we begin to see how mathematics was applied to early cryptography. We can replace letters with their equivalent place in the alphabet, then with the key word, this becomes a sequence of shift numbers. The next step is to add each key letter into the plain text letter. If the result is more than 26, we do "clock arithmetic" and subtract 26 to obtain a result between 1 and 26. What we mean here is the following: If we have the letter Y it corresponds to the number 25. If we then us the key

Metal type for newspaper printing, arranged to illustrate the Vigenère cypher, courtesy of the Braddock Letterpress Museum in Braddock, ND. Since 2016, students taking the Intro to Publishing course at NDSU typically travel to the museum to learn about moveable type and experience operating the Chandler & Price letterpress. Many pieces of letterpress equipment were donated by the Borlaug family newspapers, which were published in Washburn, ND.

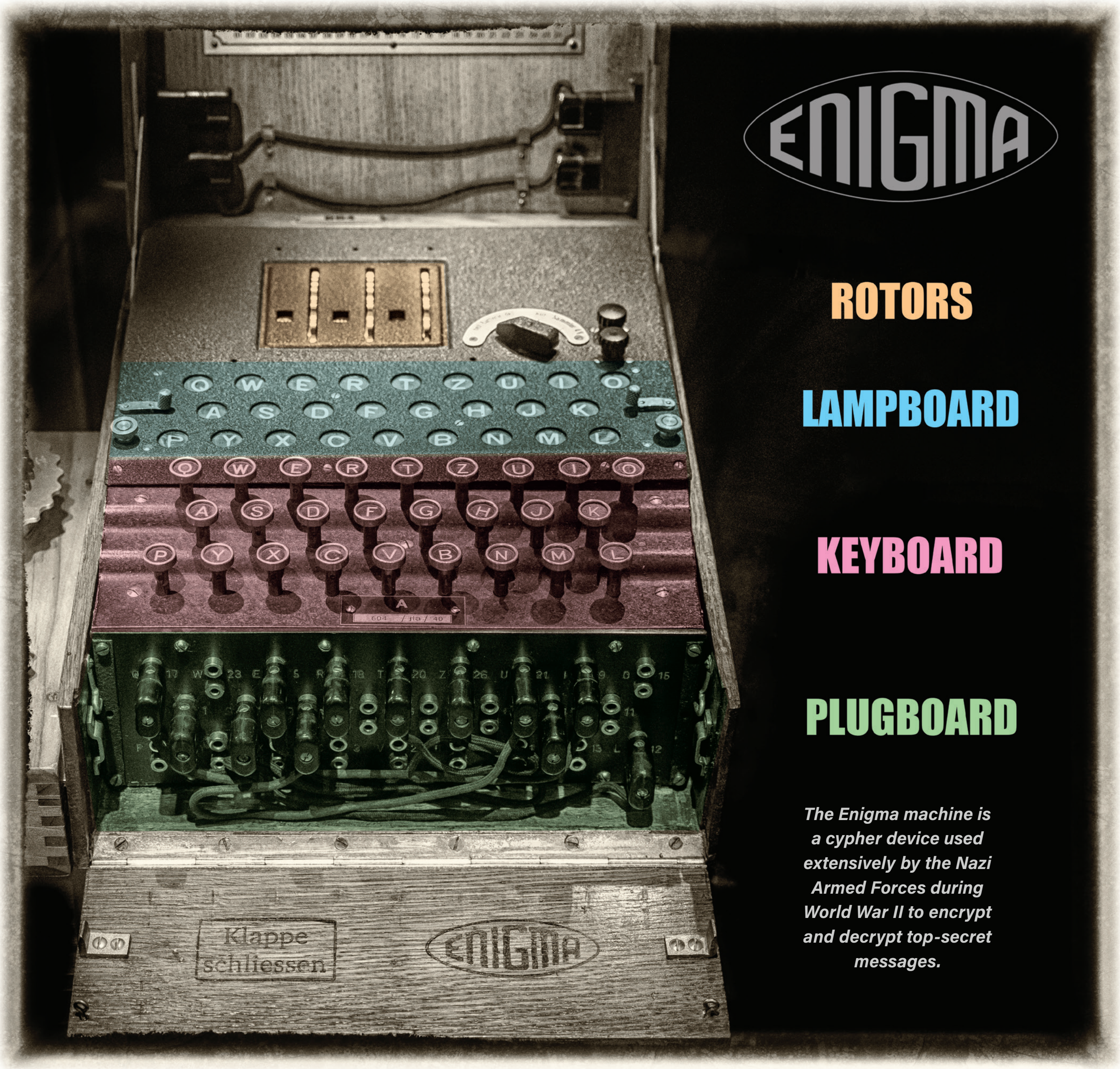
letter D, corresponding to 4 we add 4 to 25 to obtain 29. The challenge is that 29 is not in our list of 1-26. So what we do is subtract 26 to obtain 3, which is then the code letter C.

Enigma

The mathematical nature of cryptography developed through the centuries such that cyphers become entirely mathematical by World War II, during which there were significant advancements in cryptography and cryptanalysis (the study of cryptosystems). The Germans developed an entirely new machine and encryption/decryption system called Enigma. This was no ordinary substitution cypher. Enigma relied on three wheels, each of which was a permutation cypher; a plug board, which was another permutation; and a reflector.

When a key was pressed on the Enigma machine the letter was passed through the plugboard, then through each of the three permutation discs, hit the reflector, back through the permutation discs, then to a light board showing the encrypted letter. Then when the next key was pressed, the first wheel was rotated so that it aligned with the other two differently. Hence the entire system changed a bit.

The Germans thought that this code was unbreakable. But three Polish mathematicians, after a few weeks of



The Enigma machine is a cypher device used extensively by the Nazi Armed Forces during World War II to encrypt and decrypt top-secret messages.

listening to German radio communication, were able to not only break the codes but build a machine similar to what the Germans had without ever seeing it. They then went on to build a machine to break the codes called the *bomba kryptologiczna* or cryptologic bomb.

Shortly before Poland was invaded, these three mathematicians presented their work at a conference to French and British cryptographers. Thus, they passed on their knowledge of not only how the codes worked but how to break them. Alan Turing used the information from the Polish cryptographers to develop the British Bombe, the electromechanical device used to break the enigma codes throughout the war. Many historians believe that knowing how to break the codes shortened the war by at least two years.

The Cold War

A new era of cryptography began after World War II at the start of the Cold War. Information security was considered an absolute necessity by the U.S. and USSR. Both countries set up agencies dedicated to information security and warfare. Cryptography entered the academic research mainstream.

The U.S. developed the Data Encryption Standard (DES) for secret communications, which was deployed from 1979 to 2005. DES uses a 56-bit key (a string of 56 zeroes and ones) and works on block lengths of 64 bits. DES is considered insecure by modern standards because the encryption is easily broken.

Advanced Encryption Standard

In 2000, the Advanced Encryption Standard (AES) replaced DES. AES also works on blocks of data and can accept keys up to 256 bits in length. Currently, AES serves as the standard for encryption in the U.S. and many parts of the world. It is used heavily in internet communication because it is fast and secure.

Security Concerns

All the codes mentioned so far are termed symmetric cyphers, meaning that both the sender and receiver need to have the same key to encrypt and decrypt messages. This poses a challenge in that some other communication method must be used to share the secret keys since the internet might not be insecure. Embassies, for example, relied on DES for decades. Diplomats used diplomatic pouches—which by international agreement, cannot be opened at border crossings—to deliver secret keys to and from their governments to their embassies and consulates.

The underlying reason for this is a fundamental of cryptography, Kerckhoffs's principle (after a 19th-century Dutch linguist and cryptographer) states: A cryptosystem should only depend on the key, not on the algorithm used. What this means is that a secure cryptosystem should be able to share how it works with any user, including the attacker, but should still be secure as long as the key is kept secure. Another way to say this is: "Security through obscurity is not security." That is, all security systems should be secure even if publicly known. As a corollary to Kerckhoffs's principle and this statement is that the more secrets a security system has, the more vulnerabilities it also possesses.

Both DES and AES are public algorithms in that how they work is completely known. This allows for any cryptographer to study the algorithm and see if flaws can be found. A fundamental rule of cryptography is that anyone can make a system that he or she can't break, but, no matter how complex, someone else might be able to break the system.

So, DES and AES satisfy Kerckhoff's principle in that the only piece of information that is needed for the system to be secure is the key.

One-Time Pad

The ultimate in security is given by the one-time pad. Here the secret key is at least as long as the message. What we want the key to be is as random as possible, in order that an eavesdropper not only can't read the message but can't tell that it's a message in the first place—analogous to background noise in electric transmissions. The key is then used to encrypt the message letter by letter. The result, if the key indeed looks like noise, is a message that appears to be random noise. Any plain text of the same length as the encrypted text is just as likely. As an example, if we encode "truth" using a particular one time pad we might obtain the cypher text "AQHBT". Now if we know the key, we easily obtain our original message. But it turns out that without the correct key, a different key could give any other five letter word, such as "whose." As a result, the one-time pad provides the highest level of security.

Key Exchange and Public Key Cryptography

The challenge for the one-time pad is that both sides need to have obtained the same secret key somehow. In 1976, two researchers from Stanford University, Whitfield Diffie and Martin Hellman, published a paper that revolutionized cryptography and made encryption across the internet possible. In this paper, they introduced the notion of public key cryptography.

Public key cryptography is different than symmetric key cyphers (where the encryption and decryption keys are the same) in that there are two different keys, one for encryption and one for decryption. A user is then able to publish his or her encryption key that anyone can use to encrypt messages. The message is then decrypted using the decryption key or private key.

While they didn't have a public key cryptosystem, they did publish a method for two people to develop a key across an insecure channel. Using this key exchange, two users can have the same private key that an observer cannot obtain by any known method except brute force (testing all possibilities), which would take thousands of years. The two users would then use an agreed-upon symmetric algorithm like AES.

RSA

Public key cryptography became a reality with the development of a new algorithm by Rivest-Shamir-Adleman known as RSA. The math behind RSA is not terribly difficult and is accessible to an advanced high school student. However, without the secret numbers—two secret numbers (prime numbers of 200 digits or more) are chosen to generate the private key—it is very difficult to generate the private key from the public key, unless one has thousands of years of computer time available.

Elliptic Curve Cryptography

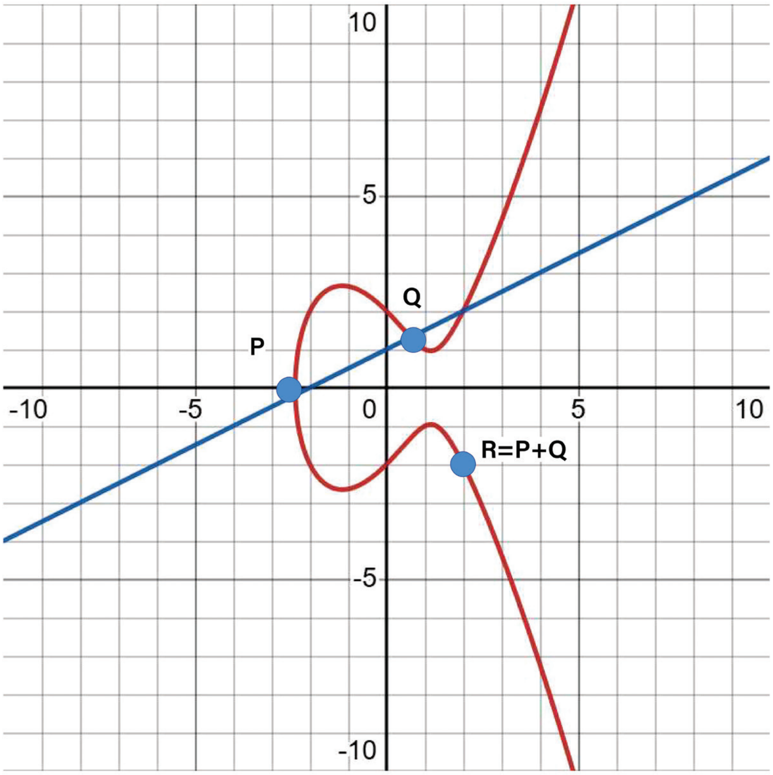
The next major advancement in public key cryptography came in the form of elliptic curves ($y^2=x^3+ax+b$). In the xy-plane, shown in the graph below, elliptical curves are well behaved, but in clock arithmetic they act somewhat randomly, which makes them quite adept at generating secret keys. Using surprisingly simple math equations, we can produce these common secret keys. This key-exchange algorithm has become the standard at many websites, including Google and Wikipedia.

The magic of elliptic curve cryptography is that the key size is significantly shorter than the RSA keys. As a comparison, an elliptic curve key of length 256 bits is equivalent to an RSA key of 4096 bits. Further, the algorithm is very fast.

Digital Signatures

One fascinating facet of all current public key algorithms is that the public key and private key can be applied in any order. This allows for signing of documents. What the user does is apply his or her private key to the document to "sign" it. Anyone can then verify the signature by applying the appropriate public key. Two users can sign the same document by applying their private keys in succession. Then again, the signatures can be verified by applying the appropriate public keys.

Elliptic Curve Cryptography: The elliptic curve, $y^2=x^3-2x+4I$, is all points (x,y) satisfying this equation. The curve (the red line) is symmetric about the x-axis because of the y^2 term. The second step involves point addition on elliptic curves: Choose two points, P and Q, and draw a line between them. One property of elliptic curves is that this then crosses the curve exactly once. Take this new point and reflect it across the x-axis to arrive at R = P+Q. This "addition" property is essential to elliptic curve cryptography. The third step involves an elliptic curve in clock arithmetic, which produces a random distribution of points that renders a specific message indistinguishable from any other message of the same length.



Bitcoin

The bitcoin algorithm uses elliptic curve cryptography in its implementation. What bitcoin is at its core is a ledger of how much bitcoin an account has. The accounts are given by public keys of the elliptic curve cryptosystem. When a user wants to spend their Bitcoin, they specify a different account and then sign the transaction with their private key. Anyone can verify this is a legitimate transaction by applying the public key to the transaction. There is more that goes into the algorithm, but this is the heart of how transactions work.

Protection vs Security & Privacy

The American public is heavily reliant on cryptography for day-to-day functions. From securely browsing the internet, to chip-and-pin transactions on debit cards, or chip-only transactions with credit cards. Further, there are many chat programs that rely on cryptography to keep the user's messages secure from eavesdroppers.

Currently, however, there is legislation under consideration in Congress, which according to many experts unintentionally puts digital privacy at risk for private citizens and the business and industry sectors.

The EARN IT Act was originally introduced in 2020 with the aim of protecting children from online sexual exploitation. Strong public opposition and pushback from human rights organizations caused the bill to be shelved. Then the bill was re-introduced to the U.S. Senate in February 2022 and soon endorsed by the National Center for Missing and Exploited Children and the National Center on Sexual Exploitation. The bill would create a National Commission on Online Child Sexual Exploitation Prevention with laudable goals.

The problem is that implementation would almost certainly grant the government access to end-to-end encryption in order to identify, track and prosecute criminals. End-to-end encryption is fundamental to privacy for email providers and security for business communications, which often involve highly sensitive data. Legislating backdoors to this encryption will allow access without notification not only to government agencies, including law enforcement, at the local, state and federal levels—but worse, the backdoors will also enable hackers to gain the same access.

In short, privacy and security in digital services and communications will be irreparably shattered. Not surprisingly, the government will be exempt from these measures. The Electronic Frontier Foundation criticized the EARN IT Act as "a direct threat to constitutional protections for free speech and expression." In a poll this July from AXIS Research, respondents identified privacy (21 percent) as the top issue Congress should focus on concerning tech-related issues. Protecting children online certainly concerns voters but ranked third at 11 percent.

The choice between privacy and protection, unfortunately, is a fundamental either/or. There is no legislative fence to land on; encryption's backdoor is open or shut, never slightly ajar.

■ *Further Reading*

If you are interested in learning more about cryptography, there are a few excellent texts available:

Serious Cryptography by Jean-Philippe Aumasson is accessible to many but has some technical details.

For those more interested in the algorithms, I recommend the classical text *Applied Cryptography* by Bruce Schneier.

The mathematics behind the algorithms is discussed in *Introduction to Cryptography with Coding Theory* by Wade Trappe and Lawrence Washington.

For more information on Kerckhoffs's principle, see this article: https://www.schneier.com/crypto-gram/archives/2002/0515.html#1

Lastly, I will be teaching a course on cryptography through the Dakota Digital Academy and Dickinson State University in the spring of 2023.

Artificial Intelligence is Transforming Our World–*Are We Ready?*

NIKOLA L. DATZOV, JD
Assistant Professor of Law
University of North Dakota

Our world is changing. Cars drive themselves. Automated grocery stores allow customers to shop without employees in the store. Drones manage and spray our farm fields. Software applications control access, temperature and lighting in our smart homes. Autonomous robots clean our houses. Voice-controlled virtual assistants help ease the burdens of many daily tasks. Facial recognition cameras help identify persons of interest in busy crowds. Imaging analysis software helps doctors provide medical diagnosis more quickly and accurately than ever.

These are just some examples of how artificial intelligence (AI) is revolutionizing our society in unprecedented ways. In fact, the United States Patent and Trademark Office (USPTO)—the government branch primarily responsible for overseeing innovation in the U.S.—expects AI to "revolutionize the world on the scale of … electricity."[i] It is worth pausing to conceptualize the level of impact at issue. Imagine our world without electricity. Whether good or bad—whether we like it or not—this is the level of change at stake in the AI revolution. Driven by massive amounts of data, often collected from individuals, AI is able to emulate human intelligence and perform tasks historically performed by people. What was once science fiction will be tomorrow's new normal. Although we have already moved past whether we *should* adopt AI into our lives, we should not overlook the important question of whether we are *ready* to adopt this quickly evolving technology.

Emerging AI applications will undoubtedly advance our technology and improve our lives. They will likely make our roads safer and our homes more comfortable, improve our food production and ease the burdens of many everyday tasks. There exists a dark side to such advancement, however, and the meteoric rise of AI technology will certainly raise many significant societal questions. There is perhaps no greater uncertainty than how AI will impact our economic growth and likely displace some of our workforce in coming decades.

Illustration by
Jerry Anderson

Much closer on the horizon, three pressing legal questions have already emerged and remain largely unanswered: First, who will be legally responsible when AI causes injury? Second, how will we protect the immense value of AI innovation? Third, how will we balance the competing interests of AI's societal benefits with its societal costs, such as reduced individual privacy? Before considering these legal gray areas—AI liability, innovation and privacy—it is pivotal to first understand the scope and the importance of specificity when addressing AI.

What Do We Mean by "Artificial Intelligence"?

Although AI is nearly ubiquitous, it has no universal definition. It is not an area of law nor a single industry. AI is a technological revolution that impacts virtually all facets of our lives. A common definition of AI refers to the capability of machines to emulate human behavior, particularly intelligence and decision making.[ii] However, this definition is certainly underinclusive in how society uses the term. Sure, artificial intelligence includes Terminators, IBM's Watson and other highly sophisticated, autonomous and (perhaps in the future) self-aware computer systems. But AI—perhaps in conflation with automation—is often used to describe much more, such as: (1) software that performs processing typically performed by humans; (2) software that uses data to provide reports; (3) fitness trackers; (4) software that uses data for predictive analytics; (5) smart thermostats; (6) software that predicts illness spread, weather or traffic; (7) hardware components for robotic systems; (8) software that understands and mimics human speech; (9) virtual assistants; (10) underlying computer algorithm designs; (11) content recommendations on streaming platforms; and (12) autonomous robotic systems. In categorizing patents, even the USPTO found no definition with adequate specificity and instead defined AI patents by identifying eight "component technologies."[iii] Given the varying definitions, AI's scope for now is defined only by the label we ascribe to it.

To be sure, AI is different from the Internet of Things (IoT), which generally refers to devices with sensors capable of gathering data and communicating over the internet. But the line between AI, IoT and mere software can become blurry. Ultimately, what becomes clear about the definition of AI is that it lacks clarity because AI's potential scope, as understood by the general public, often stretches far beyond the narrower scope ascribed by scientists and engineers.[iv]

AI's evolving and broadening nature presents challenges in measuring its impact and analyzing policy decisions. Potential liability from errors in weather forecasting software presents different considerations than errors from medical diagnostic software. Innovation in autonomous vehicle and drone technology impacts our economy differently than automated calendaring software. And the data associated with what temperature our thermostat is set to at night presents different privacy concerns than the devices in our living room listening to (and perhaps recording)[v] our conversations.

Accordingly, specificity is important. In making policy decisions, characterizing the issue merely as AI can be misleading. Yet, addressing AI policies and regulation at the micro level for each individual technology can be overwhelming and inefficient. Luckily, this is not necessary since there exists a "Goldilocks level" of specificity when addressing AI. Although, as a category, AI is far too broad to be specific, commonalities pervade its continuum. For example, like technologies can be grouped together. The key to meaningful dialogue and specificity is recognizing AI's breadth and deliberately using specificity for precisely the AI category at issue. When addressing AI, we must articulate its scope and meaning or group it only with contextually similar applications.[vi]

Is Our Legal System Ready for AI?

Our society's readiness for AI, in many ways, will be measured by the readiness of our legal system. After all, our legal system is the system of rules for what conduct society is willing to accept, how we are willing to allocate risk, and who we believe is deserving of compensation. Laws govern everything we do. Although AI will raise many questions regarding legal policy—some of which have yet to be considered—three leading questions have emerged:

First, how we will impose liability for injuries caused by AI; second, how we intend to protect and promote the innovation of AI technology; and third, how we will balance concerns for individual privacy from AI use with benefits to society as a whole.

AI Liability

"Who is responsible for this?" That question has echoed in our minds since childhood. At its core, this simple question is rooted in the fundamental notion that those "responsible" for causing harm should be required to remedy it—which most often means "pay for it." As AI continues to play an increasing role in our everyday lives, the potential for harm (and liability) seems inevitable. Self-driving cars crash, automated software applications malfunction, and AI predictions prove to be wrong. When harm results, we will once again ask, "Who is responsible for this?" Except, we will be asking that question in a new frontier where decisions might have been made by a robot (or autonomous system) instead of a human.

In the absence of a contract that answers the question, liability for such wrongdoing is governed by tort law in the U. S. The law of torts imposes liability for both intentional torts (when the wrongdoer's conduct was intentional) and negligent torts (when an actor had no intention of causing harm but did so in a way that society views as falling below a "reasonable" standard of care). Negligence (unintended harm) is the most common form of tort liability and will likely continue to be in the context of AI, where the vast majority of AI is likely to be programmed to avoid causing harm. To demonstrate liability for negligence, a party must generally demonstrate four elements: First, the defendant owed a duty to the plaintiff; second, the defendant breached a duty to the plaintiff; third, the defendant's actions were the cause (both "actual" and "proximate") of the plaintiff's injury; and fourth, the plaintiff sustained some harm or injury.

In a negligence lawsuit involving AI, the plaintiff will be obvious: the person who suffered the harm. But who will the defendant be? The AI system? The person who developed the AI system? The company that developed the AI system? The company that sold the AI system? The person who operated the AI system? The list is limited perhaps only by the creativity of the plaintiff's attorney and whatever legal limits exist for liability under tort law.

Given the clear focus of the analysis on the *defendant*'s actions to prove a negligence claim, it is imperative to name the right party as a defendant. As a matter of practice, a plaintiff lawyer's creativity to seek a meaningful recovery for the client is frequently guided by the opportunity to sue wealthy parties, often a company. Why? Because they are most likely to result in a payment to the plaintiff. Obtaining a $10 million judgment can quickly become a Pyrrhic victory, when the defendant found liable has no assets (insurance or funds) to satisfy the judgment. In such a case, the plaintiff wins the legal claim, yet remains uncompensated. Worse, since many personal injury cases are litigated on a contingency basis (where the plaintiff's lawyer is compensated only if the plaintiff recovers), a dim prospect of actual payment might result in difficulty even obtaining a lawyer. For some accidents, this might not pose a significant concern. In most fender-benders, for example, finding a party liable results in compensation either through the insurance company or the responsible party, who is likely to have assets to satisfy a small judgment. But raise the stakes to a single plaintiff with very significant injury (for example, a child killed by a self-driving car or a plaintiff misdiagnosed by medical software) or thousands of plaintiffs with relatively minor harm (for example, a smart thermostat that turns off the heat to thousands of homes or a digital assistant that mistakenly orders items online[vii]) and the potential for under-compensation becomes real, particularly against an individual or a small, underinsured company with few assets.[viii]

Devising a general rule as to which party should be held liable anytime AI causes harm is difficult. Like any negligence case, context is critical, and the liability of the actor will depend on the particular circumstances of the case, as well as what led to the harm. The questions central to the inquiry of liability are likely to include: Whose conduct fell below society's expectations, and was the harm foreseeable from the conduct at issue? Yet, it doesn't take a lawyer to appreciate the difficulties raised by negligence elements for imposing liability for AI-caused harm.

NORTH DAKOTA CENTURY CODE ANNOTATED
2012 REPLACEMENT
4A
FISH
SAFETY
NORTH DAKOTA CENTURY CODE ANNOTATED
2002 REPLACEMENT
4B
NORTH DAKOTA CENTURY CODE ANNOTATED
2017 REPLACEMENT
4C
NORTH DAKOTA CENTURY CODE ANNOTATED
2016 REPLACEMENT
5
NORTH DAKOTA CENTURY
NOR DAKO CENT COD ANNOT
201 REPLACE
7E

Illustration by Jerry Anderson

For many obvious reasons, a suit against an AI system itself is implausible, at least until AI systems start gaining personhood[ix] and owning property. When a dog bites someone, the plaintiff doesn't sue the dog.

Also, negligence suits against AI developers are far from guaranteed to provide recovery because problems might arise with demonstrating that the developer owed a duty to the plaintiff, if the software is used in a way not intended by the developer or harms someone who was not anticipated to be impacted by the software. An additional concern might be proving that the developer was the cause of the harm, if the AI system caused harm in an unexpected and unforeseeable way.

AI systems can often be a "black box" due to the inability to know exactly how the system operates or makes its decisions. The more complex the thinking of the AI system, the further removed the developer is from foreseeability, and the less likely there is to be liability. Similarly, a reseller of an AI system might not have done anything unreasonable simply by providing a product or service developed by someone else. As such, there may be a need to rethink the applicability—or at least the scope—of foreseeability in our traditional analysis of negligence law when it comes to AI liability.

An alternative avenue to liability against AI systems may be based on strict liability—a tort claim that imposes liability regardless of whether the defendant's actions were intentional or reasonable. But strict liability laws are limited to very specific contexts, such as animals, abnormally dangerous activities and products liability. Although the discussion has spanned decades, it is still far from clear whether software constitutes a "product" that is subject to strict products liability.[x] Since AI provided by a party primarily—sometimes exclusively—comprises software, strict liability currently might not extend to AI.

However, even if an AI system does not fit within any of these categories, expanded strict liability laws (and accompanying insurance policies) may emerge as the leading way to govern the compensation of harm caused by AI systems. Importantly, imposition of liability without intent or negligence has drawbacks and requires careful consideration, especially regarding corporate willingness and ability to absorb such risk into business practices. A broader scope of insurance coverage leads to more expensive insurance and a higher cost of doing business, which might prohibit or discourage some AI uses and developers.

So, when the familiar question "Who is responsible for this?" arises in the context of the new AI frontier, we can take comfort in the robust, time-tested legal framework that we can look to for answers. Yet, that comfort may be misplaced. Tort law is largely shaped by constantly changing policy decisions about how our society chooses to allocate risk and provide compensation. Moreover, tort law is primarily governed by state law, which creates the very real potential for inconsistent laws and policies across different states. In the context of AI's emerging issues, the existing legal framework remains largely uncharted as to where these policy lines should be drawn. Absent legislation on AI liability, the boundaries for responsibility in this new frontier will continue to develop through common law (litigating individual cases in the courts). Since the development of common law takes significant time and a willingness for parties to take on the increasing costs of litigation, the law on AI liability could lag far behind society's fast-paced adoption of AI.

Protection of AI Innovation

The boom in AI development has seen an enormous amount of innovation in just the last decade. For example, "[t]here were 10 times as many AI patent applications published in 2019 as in 2013" and "[t]he same time period saw an almost four-fold increase in granted AI patents."[xi] Not surprisingly, AI's immense value has created a significant legal battleground for exploiting and protecting AI innovation. When it comes to leveraging AI innovation, individuals and companies have two key questions to consider: Do I have the legal right to do what I would like to do, and do I have the legal right to exclude others from doing it. The regulation of these legal questions falls squarely in the domain of intellectual property (IP).

IP refers to intangible property—"creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce."[xii] IP law is comprised of four core legal areas: patents, trade secrets, copyrights and trademarks. Patent law, in particular, is a critical way to protect innovation in the U. S. The scope of what can be patented is quite broad: "[A]ny new and useful process, machine, manufacture or composition of matter, or … improvement thereof" is eligible for a patent, provided that the applicant can satisfy all other requirements in the statute.[xiii] An owner of a patent enjoys a powerful monopoly to exclude others in the U.S. from making, using, offering to sell or selling the patented invention.[xiv]

An alternative for protecting innovation—particularly innovation that is kept secret—is trade secret law. Governed by both federal and state law, trade secret law protects "all forms and types of financial, business, scientific, technical, economic or engineering information," but only if the owner has taken reasonable measures to keep such information secret and the information "derives independent economic value … from not being generally known."[xv] Although trade secret law does not protect against reverse engineering or independent discovery, it prohibits others from "misappropriating"—acquiring or disclosing—a trade secret through "improper means."[xvi]

Copyright law protects original works of authorship fixed in tangible form—such as literary works, musical works, motion pictures, sound recordings, architectural works—from unlawful reproduction and distribution.[xvii] It does not protect, however, any "idea, procedure, process, system, method of operation, concept, principle, or discovery."[xviii] Thus, for example, copyright law might protect against the reproduction of the particular way in which a cooking recipe is expressed, but it would not preclude others from using or sharing the underlying process described in the recipe.

Trademark law has a narrower scope in protecting AI innovation. A trademark is "any word, name, symbol or device, or any combination thereof" used to distinguish one's goods and indicate the source of goods.[xix] Simply put, it is "how customers recognize you in the marketplace and distinguish you from your competitors."[xx]

The importance of IP and its value in today's world cannot be overstated. Gone are the days when most companies' value was tied to the buildings they owned and the widgets they made. According to recent reports, "intangible assets"—a very significant portion of which are IP rights—are "now responsible for 90 percent of all business value," as opposed to just 32 percent in 1985.[xxi] With so much value now tied to IP rights, the competition for IP innovation and ownership has never been greater. Moreover, the demand—even dependence—on owning IP has amplified the importance of the delicate balance at the center of patent and copyright law.

A core principle underlying patent and copyright laws is that they provide strong incentives for individuals and companies to devote resources and time to innovation by granting them exclusive rights as a reward for their investment. However, as we grant more IP rights to individual inventors and authors, the more we limit the public's use and access to those rights. For example, granting a broad patent on drone technology leaves less for society in that same space due to the powerful monopoly to exclude others from using or selling the patented invention. As the U.S. Supreme Court has explained, "monopolization of [basic tools of science and technology] through the grant of a patent might tend to impede innovation more than it would tend to promote it."[xxii] Additionally, the exertion of broad IP rights can provide significant (and sometimes improper) leverage against competitors in both the marketplace and litigation.

The debate on the appropriate scope of IP rights to promote, rather than stifle, innovation is far from new. And that debate is certain to carry through into the policy discussions surrounding the AI revolution. Recently, the National Security Commission on Artificial Intelligence asserted that "[t]he United States lacks the comprehensive IP policies it needs for the AI era and is hindered by legal uncertainties in current U.S. patent eligibility and patentability doctrine."[xxiii] Others believe that the exponential growth in AI patents,[xxiv] AI publications[xxv] and AI investment[xxvi] demonstrates tremendous promise for AI innovation under the current legal framework. Although many views exist on where to draw legal boundaries for protecting AI IP, everyone seems to share the view that the future answers to these questions will have tremendous importance for AI innovation in the U.S.

As the historical debate on balancing IP rights takes center stage in the emerging AI space, a related, but perhaps even more complex, question has developed with it. While AI IP has traditionally meant the inventions and artistic works developed and created by individuals and companies in the realm of AI, as AI systems become more sophisticated, AI has moved from *being* intellectual property to *generating* intellectual property. For example, on July 29, 2019, the USPTO received a patent application listing a single non-human inventor for an "[i]nvention generated by artificial intelligence."[xxvii] This raises the unique and novel question of who owns IP generated by AI.

Although not fully settled, current U.S. patent law appears not to allow AI to own a patent or to be listed as an inventor on a patent. In answering the question whether an "artificial intelligence machine [can] be an 'inventor' under the Patent Act," a federal district court (in the companion litigation to the above patent application) recently held that "the clear answer is no."[xxviii] In the appeal of that case, the USPTO continued to maintain that under "[t]he plain language… [of] the Patent Act… – only a human being can be an 'inventor.'"[xxix] Importantly, though, some other countries have taken a different approach and permitted AI to be listed as an inventor on a patent.[xxx]

Addressing a similar question, copyright law has been interpreted not to allow AI to be listed as an author of an artistic work. Although the Copyright Act does not define "author," the Register of Copyrights has identified in its administrative manual that "[t]o qualify as a work of 'authorship' a work must be created by a human being."[xxxi] "Works that do not satisfy this requirement are not copyrightable."[xxxii] The Copyright Review Board recently reaffirmed this view of the law when it denied copyright registration for an AI-generated artwork.[xxxiii] Court decisions have reached similar holdings that non-humans are not authors for purposes of copyright law.[xxxiv]

These legal holdings have intensified the question of who owns AI-generated inventions and artistic works,

Illustration by Jerry Anderson

With technology's pervasiveness in our lives, the reality—whether we like it or not—is that we create trails of data in almost everything we do.

if the AI system does not meet the legal requirements to be an inventor or author. Is it the company that owns the AI at the time of invention/creation? The company that originally developed the AI? Or does the invention/artistic work fall into the public domain with no private owner? These questions are far from only theoretical or academic. For individuals and companies who use and rely on AI technology in their business, the answer to ownership of AI-generated inventions and artistic works may have tremendous impact on the value of their business.

Privacy of AI Data

Quality data is extremely important to AI innovation. In fact, AI depends on data to function. The Economist recently proclaimed, in an article title, that "The World's Most Valuable Resource Is No Longer Oil, But Data."[xxxv] AI systems that provide reports or predictions utilize and analyze large amounts of data to achieve their desired function. Even more importantly, more sophisticated AI systems, such as those making autonomous decisions, depend on data to learn how to differentiate and identify patterns and objects. For example, to train AI software to recognize a picture of a cat, the developer can utilize a large dataset of cat pictures to allow the AI system to learn what a cat picture looks like. Once the AI system has reviewed a sufficient number of pictures, it can rely on its trained algorithm to autonomously recognize a picture of a cat from a group of pictures. Without quality data, however, it would be virtually impossible for sophisticated AI systems to achieve their objectives.[xxxvi]

In some industries, it can be difficult to obtain useful data for AI development. For instance, in developing medical diagnostic software, access to medical imaging datasets can be very limited.[xxxvii] In many other areas, however, access to data is plentiful—at least for some (often larger) companies. For example, Amazon has access to an immense amount of data on the shopping habits and trends of most Americans. With technology's pervasiveness in our lives, the reality—whether we like it or not—is that we create trails of data in almost everything we do. Your phone tracks where you go and how long you stay there. Your browser and social media applications track your internet footprints. Your fitness tracker records your health and sleep patterns. And cars not only monitor your driving habits but now check your level of attention to the road.

Abundant access to an increasing amount of user data provides opportunities for tremendous societal benefits. For instance, location data from phones helps find missing persons and solve crimes, internet activity provides convenience in quickly finding relevant information and products, social media posts help support societal movements, digital health devices improve our health and alert us to concerns, and driving data helps reduce accidents and create safer roads. As AI applications become more sophisticated, their impact and potential to improve our society will continue to expand.

However, there is a dark side to constantly sharing data about ourselves. Unfortunately, not all data is used for public good, much less for the benefit of individuals. In fact, much of it is collected for commercial gain. Unchecked, data use in AI algorithms has the potential to hide biases and perpetuate biased decisions without adequate oversight.[xxxviii]

In addition, everyone has different expectations of privacy because not everyone is willing to share private data with the world, even for the greater good. Have you ever run an internet browser search for a product only to be unsuspectingly spammed with advertisements for the same product minutes later? Such targeted advertising occurs based on data left behind in your internet footprints. Surprising as it may be, the collection and sharing of data often happens behind the scenes, so that people may not even recognize what data they are sharing. Although companies often provide disclosures about the data they collect and how they use it (usually explained in user agreements), not every user takes the time to read those lengthy documents. Those who do may not fully understand them and likely would be powerless to change them.

Even further, some public or self-disclosed data simply requires no user permission. Take into account that data can often be shared and sold—not to mention hacked or stolen—and it becomes nearly impossible to understand how your private data is being used, much less predict where it will go. Since individuals can be reidentified even from "anonymized" data, removing identifying information in large datasets offers limited protection. Some companies now offer products that help keep data private,[xxxix] but much of the control still lies in the companies that collect, store and use the data. Thus, the most meaningful protection for individual privacy will have to come from the laws regulating those companies.

In 2018, the European Union passed a comprehensive data protection law: the General Data Protection Regulation (GDPR).[xl] This regulation applies not just to companies in Europe but to anyone—even those not in the EU—who "process the personal data of E.U. citizens or residents, or … offer goods or services to such people."[xli] So, if a hotel in Fargo hosts Europeans or a business in Bismarck sells products to Europeans, that venue or company might be subject to the regulation's requirements. The GDPR provides a "compliance checklist" for U.S. companies.[xlii] The definition of "personal data" under the GDPR is very broad and includes "any information that relates to an individual who can be directly or indirectly identified," such as "[n]ames and email addresses… [l]ocation information, ethnicity, gender, biometric data, religious beliefs, web cookies and political opinions."[xliii] "Processing" data likewise carries a very broad definition and includes "[a]ny action performed on data, whether automated or manual," such as "collecting, recording, organizing, structuring, storing, using, erasing."[xliv] The penalties for violating

Illustration by Jerry Anderson

the GDPR can be very significant—up to €20 million or 4 percent of global revenue (whichever is higher)—in addition to damages that individuals can seek as compensation for improper data use.[xlv]

Conversely, the U.S. does not currently have a similar federal law that provides broad protection for individual data. While federal law provides protection for certain types of data—health and financial information, for example—the large gaps in privacy laws are governed by a patchwork of state laws[xlvi] that provide only scattered protection. In fact, only a few states currently offer broad data privacy laws for their citizens. As one example, the California Consumer Privacy Act—which protects only California residents—gives consumers: (1) the right to know what personal information businesses collect about them, (2) the right to delete certain personal information collected from them, and (3) the right to opt-out of the sale of their personal information.[xlvii] The scope of personal information includes "name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about your preferences and characteristics."[xlviii] The act's requirements apply to "for-profit businesses that do business in California" and meet certain threshold conditions.[xlix] Many other states have recently considered legislation to address data privacy concerns, but the scope of protection and likelihood of such legislation materializing into law varies significantly. For example, in North Dakota, a data privacy bill that would have prohibited the sale of "a user's protected data to another person unless the user opts-in to allow the sale" was presented during the 2021 Legislative Assembly but failed to pass, after a 12-1 committee vote recommended it be rejected.[l]

Undoubtedly, as the use of automation and AI systems increases, so will the need for meaningful access to data, which will increase data's value. Although security, transparency and privacy are not incompatible with data sharing or advancing AI innovation to improve society, as AI implementations begin to further impact every facet of our lives, it will be imperative to consider appropriate measures to ensure a balance between access to information and respect for individual privacy. Some of the key issues to be addressed are likely to include requirements for safely storing private data, restrictions on the transfer of data, meaningful opportunities for users to choose which data they share, and the availability for users to seek a remedy when their data is misused. As highlighted above, the conversation on these issues has only just begun.

The advancement of AI in the coming decade will revolutionize our world in unprecedented ways. This will undoubtedly offer many benefits to our society: Travel has the potential to become cheaper and safer; healthcare is poised to become more advanced, more accessible and more accurate; and automation could significantly ease many burdens in everyday life. As these changes unfold, however, important legal issues surrounding AI liability, innovation and privacy will arise that impact our society in significant ways. Although there exist no easy answers on these policy issues, it will be pivotal to consider the application of our existing legal framework to this new AI frontier before the unanswered legal issues impact our society on a larger scale. Without further research and discussion on these topics, our expansive adoption of AI could outpace our readiness to responsibly and appropriately integrate it into our society. ▣

[i] U.S. Patent and Trademark Office, "Inventing AI," 2 (2020), https://www.uspto.gov/sites/default/files/documents/OCE-DH-AI.pdf.

[ii] https://www.merriam-webster.com/dictionary/artificial%20 intelligence.

[iii] USPTO, *supra* note i at 3.

[iv] More specific terms, such as machine learning and deep neural network, which are subsets of AI, provide better clarity regarding the meaning of the technology at issue. However, they do not resolve the ambiguity surrounding the use of the broader concept of AI.

[v] *See, e.g.*, Matt Day, Giles Turner and Natalia Drozdiak, "Thousands of Amazon Workers Listen to Alexa Users' Conversations" (Apr. 11, 2019), https://time.com/5568815/ amazon-workers-listen-to-alexa/.

[vi] It may seem contradictory to emphasize the importance of specificity in making policy decisions relating to AI and then to discuss AI generally in this article. But the focus of this article is not to offer recommendations on good AI policy for any specific issue or AI technology; instead, it is to highlight the important questions that will need to be addressed in each of those policy decisions with regard to specific AI technologies. Those questions transcend all types of AI.

[vii] *See, e.g.*, Maham Abedi, "Amazon Echo mistakenly orders cat food after hearing TV commercial" (Feb. 14, 2018), https://globalnews.ca/news/4025172/amazon-echo-orders-cat-food-tv-commercial/.

[viii] Many of the companies leading AI development are large companies that would not raise such concerns. However, if liability does not extend to such companies, companies with fewer assets that were involved in the development of the AI product (such as a joint development) could become the only viable party to hold liable.

[ix] In 2017, an AI system granted citizenship by Saudi Arabia became the first robot to be given personhood. *See* Emily Reynolds, "The agony of Sophia, the world's first robot citizen condemned to a lifeless career in marketing" (Jan. 6, 2018), https://www.wired.co.uk/article/sophia-robot-citizen-womens-rights-detriot-become-human-hanson-robotics.

[x] *See* Bryan H. Choi, "Crashworthy Code," 94 Wash. L. Rev. 39, 53 (2019) ("[N]one of those arguments are new, and they have long failed to move any court to extend products liability law to software.").

[xi] *See* Center for Security and Emerging Technology (CSET), "Patents and Artificial Intelligence: A Primer," 2 and 13 (2020), https://cset.georgetown.edu/wp-content/uploads/CSET-Patents-and-Artificial-Intelligence.pdf.

[xii] "What is Intellectual Property?", World Intellectual Property Organization, https://www.wipo.int/about-ip/en/.

[xiii] 35 U.S.C. § 101.

[xiv] *See* 35 U.S.C. § 271(a).

[xv] *See, e.g.*, 18 U.S.C. § 1839(3).

[xvi] *See* 18 U.S.C. § 1839(5) and (6).

[xvii] *See* 17 U.S.C. §§ 102, 106.

[xviii] *See* 17 U.S.C. § 102(b).

[xix] 15 U.S.C. § 1127.

[xx] "What is a trademark?", USPTO, https://www.uspto.gov/trademarks/basics/what-trademark.

[xxi] https://www.oceantomo.com/intangible-asset-market-value-study/; *see also* https://www.aon.com/getmedia/60fbb49a-c7a5-4027-ba98-0553b29dc89f/Ponemon-Report-V24.aspx

[xxii] Mayo Collaborative Servs. v. Prometheus Lab'ys, Inc., 566 U.S. 66, 71 (2012).

[xxiii] National Security Commission on Artificial Intelligence, "Final Report," 12 (2021), https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[xxiv] USPTO, *supra* note i at 5; *see also* CSET, *supra* note xi at 13.

[xxv] Human-Centered AI Institute, Stanford University, "Artificial Intelligence Index Report 2021," 18 (2021), https://aiindex.stanford.edu/wp-content/uploads/2021/11/2021-AI-Index-Report_Master.pdf.

[xxvi] CSET, "Tracking AI Investment," 8 (2020), https://cset.georgetown.edu/wp-content/uploads/CSET-Tracking-AI-Investment.pdf.

[xxvii] The USPTO denied the application and refused to grant a patent. *See Decision on Petition*, https://www.uspto.gov/sites/default/files/documents/16524350_22apr2020.pdf

[xxviii] Thaler v. Hirshfeld, 558 F. Supp. 3d 238, 240 (E.D. Va. Sept. 2, 2021), *appeal pending*, No. 21-2347 (Fed. Cir. Sept. 24, 2021).

[xxix] *Thaler*, No. 21-2347, Dkt. No. 34 at 17.

[xxx] South Africa was the first jurisdiction to grant Thaler's patent application. Australia's federal court initially held that inventors need not be human, but a later decision by the full federal court reversed the holding. The other jurisdictions that have examined the application, such as the European Patent Office, have denied Thaler's application.

[xxxi] Compendium of U.S. Copyright Office Practices § 313.2, *available at* https://www.copyright.gov/comp3/chap300/ch300-copyrightable-authorship.pdf.

[xxxii] *Id.*

[xxxiii] https://www.copyright.gov/rulings-filings/review-board/docs/a-recent-entrance-to-paradise.pdf

[xxxiv] *See, e.g.*, Naruto v. Slater, 2016 WL 362231, at *4 (N.D. Cal. Jan. 28, 2016), *aff'd*, 888 F.3d 418 (9th Cir. 2018) (holding that a six-year-old crested macaque "is not an 'author' within the meaning of the Copyright Act").

[xxxv] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[xxxvi] Use of data to train AI does not itself provide ownership or protection for the data. As noted in the above section, whether a party can protect data it uses is a separate question governed by intellectual property law and contract law.

[xxxvii] *See* Edmund L. Andrews, "The Open-Source Movement Comes to Medical Datasets" (Aug. 2, 2021), https://hai.stanford.edu/news/open-source-movement-comes-medical-datasets.

[xxxviii] *See, e.g.*, Jeffrey Dastin, "Amazon scraps secret AI recruiting tool that showed bias against women" (Oct. 10, 2018), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

[xxxix] *See, e.g.*, https://duckduckgo.com/.

[xl] *See* https://gdpr.eu/what-is-gdpr/.

[xli] *Id.*

[xlii] https://gdpr.eu/compliance-checklist-us-companies/.

[xliii] *See supra* note xl.

[xliv] *Id.*

[xlv] *Id.*

[xlvi] *See* https://iapp.org/resources/article/us-state-privacy-legislation-tracker/#.

[xlvii] See https://oag.ca.gov/privacy/ccpa.

[xlviii] *Id.*

[xlix] *Id.*

[l] *See* https://www.legis.nd.gov/assembly/67-2021/bill-actions/ba1330.html.

Committed to the Fight?

Military Service & the Social Contract

USAF MAJ. GEN. (RET.) ROBERT H. LATIFF, PHD

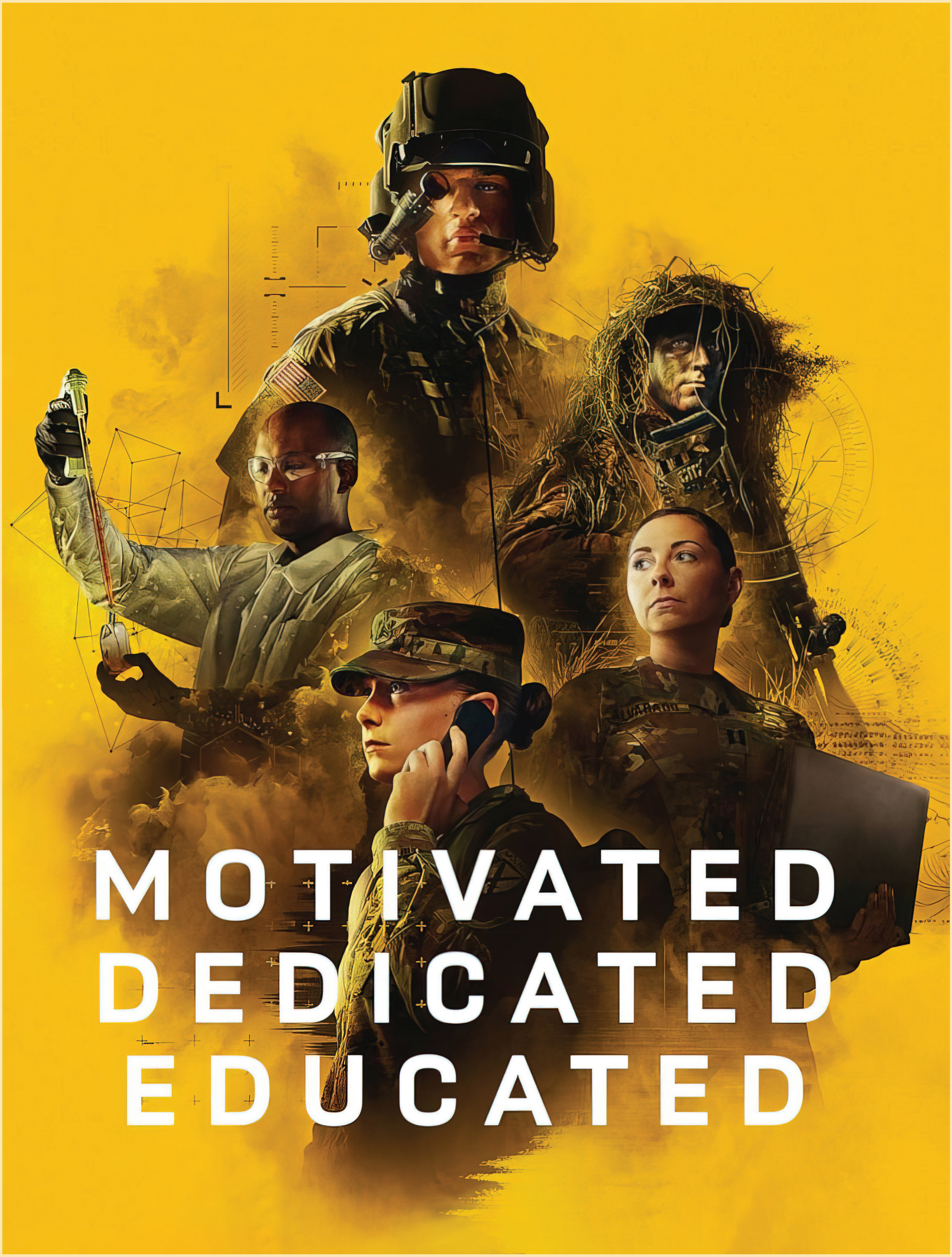
During its heyday, when ancient Rome confronted a crisis, it could call upon its citizens who felt a personal stake in the success of the empire and would willingly come to its defense. Citizens had rights but also accepted that they had duties and responsibilities. Today, in the United States, while citizens expect much of their government, they are willing to provide little in return. It seems many Americans are unwilling to satisfy their part of the "social contract" about which political philosophers, especially Thomas Hobbes, John Locke and Jean-Jacques Rousseau, wrote about as essential to a successful society.

When asked in the 2018 election cycle, an astounding 40 percent of American voters did not even know the U.S. was still fighting in Afghanistan. While the American public reveres its military and tends to be quite militaristic and eager to employ our first-rate forces around the world, most individuals do not want to be a part of it. Surveys of 18- to 29-year-olds indicate that, while a majority support the use of military forces to respond to various crises, only 15 percent have a willingness to serve in the military.

The public is happy to let someone else fight the politicians' wars, but the social contract should require something of both parties: the government and its citizens. One sure way to do that would be to force citizens to confront issues of war and peace by requiring them to participate in them.

The Other One Percent

The burden of nearly two decades of wars around the world has been borne by approximately one percent of the population. While the all-volunteer military has been off fighting endless wars, the rest of the eligible population has immersed itself in consumer goods, social media, entertainment and other quotidian interests.


MOTIVATED
DEDICATED
EDUCATED

The younger generations in particular—the ones who would and should be, and historically have been, asked to bear the burden of defending the nation—are instead playing in the ever-increasing digital universe. Clearly, immersing current and future generations in reality, especially in training for the most disruptive reality of all, kinetic and cyber war—both of which have devastating physical world effects—is becoming increasingly urgent. It just seems morally wrong to ask such a small fraction of the population to place their lives at risk on behalf of the rest of us, while we collectively give them little or no place in our daily lives and thoughts.

Not only is it unfair for the public to depend on such a tiny segment of the population to fight its frequent wars, but it also puts a worrisome distance between the interests of the country and the loyalties of the armed forces. When the Roman Empire grew, the army could no longer be demobilized after a crisis, only to be remobilized at the next crisis. As a result, the government replaced the conscript army with an all-volunteer force. Because they expected recompense after their contracts ended, their loyalty was to their commanders, not to Rome. This is not to imply that such is the case with our current military. As a professional organization with minimal connection to the public it is supposed to serve, however, the military must by necessity at least be concerned with, and act in ways to perpetuate, its continued existence and relevance. One way to demonstrate that relevance is to fight wars.

As a result of the all-volunteer force and the lack of a requirement to serve, military issues and issues of war have mostly faded from the American consciousness. It is doubtful that, if after 9/11 we had implemented a draft, the generation susceptible to it would have put up with two decades of being conscripted to, say, ensure that the ineffective Iraqi or Afghan militaries could rely on American troops for support. Instead, an all-volunteer military allowed successive U.S. administrations carte blanche to wage war for the most part removed from Americans' concern.

The volunteer military has not reduced war but instead facilitated easier commitment of U.S. troops to conflicts abroad. With little connection to the institution, and no threat of military service, Americans have decreased their attention to foreign affairs, helping to explain the persistence of the "forever wars" in Iraq and Afghanistan, even as Americans did not support them in popular polls. The all-volunteer force has lowered democratic interest in and control over the foreign policy agenda. The end of the draft severed most Americans' obligations to the military. To avoid endless wars in the future, we must move the issues of war and peace from the periphery of our national discourse to its center.

Mandatory Military Service

So how do we fix the situation?

The simplest solution—if we are going to be tempted to continue fighting endless wars—might be for the U.S. to have some form of conscripted service. More to the point, perhaps, if we had mandatory military service for everyone, we might be less willing to fight those endless wars in the first place. We should seriously consider reinstating the draft.

Amy Shafer wrote in Slate in 2017 that perhaps an annual reauthorization of the use of military force should be tied to the revival of the draft, the thinking being that if Congress failed to pass a new authorization, the draft would be reinstated. For sure, such an arrangement would force this issue into the public's thinking.

The first uses of conscription—forcing individuals to serve in the military—date back to the Roman era and to feudal times. The practice developed substantially during the Napoleonic era and spread quickly throughout Europe in the early years of the 19th century. In the U.S., conscription was first used by both the North and the South in the Civil War, and again in the Spanish-American War, World War I, World War II, the Korean War and the Vietnam War.

Conscription was ended in the U.S. in 1973. Since then, America has relied on an all-volunteer military that it has used repeatedly in at least 10 major operations and dozens of lesser ones. At least 60 countries around the world have some form of conscription, among them several of our allies and our primary state adversaries, Russia and China.

National Commission Report

The National Commission on Military, National and Public Service, created by Congress in 2017, conducted a comprehensive review of such service. Among other things, the commission found what most of us already know: Military service is a responsibility borne by few, public service needs an overhaul, and civic knowledge is lacking. No surprises there.

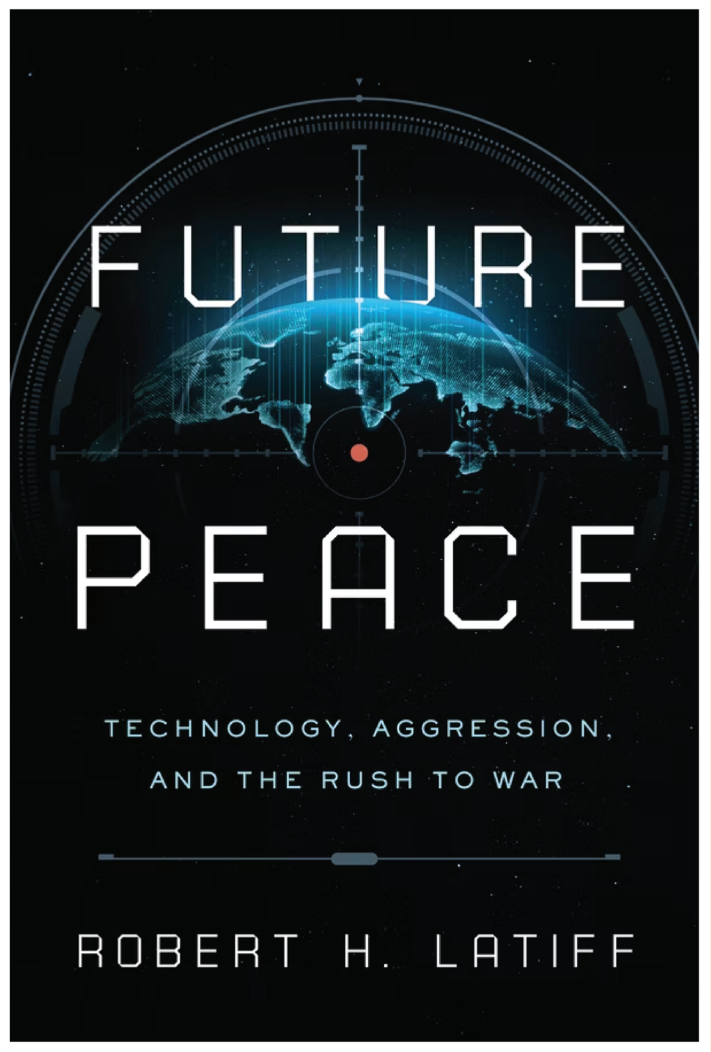
Also discovered, however, was that Americans are willing to consider a variety of options to encourage or require some form of service of all citizens. The commission considered ways of requiring all citizens to serve, with varying ways to fulfill the requirement. The final report with more than 100 recommendations was issued over a year ago.

The commission made an urgent plea to Congress and the president. But the Congressional committee with the authority to act on those recommendations never considered them in a public forum. Instead, the commission disbanded, and, sadly, Congress never seriously considered the commission's recommendations for the purpose of enacting legislation.

Conscription Need vs Politics

Conscription became a topic of renewed interest and concern with the U.S. drone strike in January 2020 that killed a top Iranian military official, followed by Iranian military retaliation and the promise of further retribution. Draft-age men across the country expressed growing concern about a war in the Middle East that would require more troops than the all-volunteer force could provide.

Recent events in Ukraine and the possibility of a ground war in North Atlantic Treaty Organization (NATO) territory have raised questions about Article 5 and the common defense among NATO allies. Article 5 of the North Atlantic Treaty committed the organization's 30 members, including the U.S., to agree that "an armed attack against one or more of them in Europe or North America shall be considered an attack against all of them."[1] What would be the role of American forces in such a situation?



***Future Peace: Technology, Aggression, and the Rush to War,* by Robert H. Latiff, University of Notre Dame Press, 2022.**

While a revival of the draft would be politically controversial, the way Americans react to such events clearly demonstrates how quickly public opinion could be engaged to make a difference in the politicians' proclivity to war. ▣

[i] "In Honor of the 60th Anniversary of the North Atlantic Treaty Organization, Summit Meeting of NATO Heads of State and Government," April 3-4, 2009. Accessed February 14, 2022: https://www.nato.int/nato_static_fl2014/assets/pdf/history_pdf/20161122_E1-founding-treaty-original-treaty_NN-en.pdf

Overlooked Security Challenges in Electric-Vehicle Charging Infrastructure

ASAD WAQAR MALIK, PHD
Postdoctoral Scholar, Department of Computer Science, North Dakota State University

ZAHID ANWAR, PHD
Associate Professor, Department of Computer Science, North Dakota State University

In October 2021, a Tesla with Autopilot enabled was involved in a collision. The vehicle in front of the Tesla stopped suddenly and, as the investigation by the Netherlands Forensic Institute showed, the driver reacted in time to the warning system and took back control of the car. The crash still occurred because the Tesla's Autopilot miscalculated and followed the vehicle in front too closely, especially considering traffic density.

After the accident, the investigation team decided to hack into the vehicle's data storage system rather than rely on data from Tesla in order to ensure the objectivity of their findings. Not only were they able to successfully decrypt the pre-crash data**.** Interestingly, they also discovered that Tesla electric vehicles (EVs) store much more information than was publicly known, such as the vehicle's speed, positions of the acceleration pedal and steering wheel, and braking behavior. This data would greatly help forensics experts investigating a fatal accident, especially in a criminal inquiry.

In April 2022, researchers at the University of Oxford and Armasuisse S+T identified a new cyberattack that enables hackers to remotely disrupt the EV charging process.[i]

In May 2022, thieves stole two cars in a neighborhood in South Austin, Texas, without having access to the car keys by using nothing more than a portable digital hacking device.

EVs and the EV charging ecosystem have become a playground for hackers—both legal and illegal—since safety and privacy policies are in their infancy. Upstream Security's 2021 Automotive Cybersecurity Report noted a 225 percent increase in vehicle cyberattacks on cars from 2018 to 2021 and projected that cyberattacks will cost the automobile industry $505 billion by 2024.[ii] As EVs increase in popularity, security and privacy challenges need to be addressed before the EV ecosystem can achieve mainstream adoption.

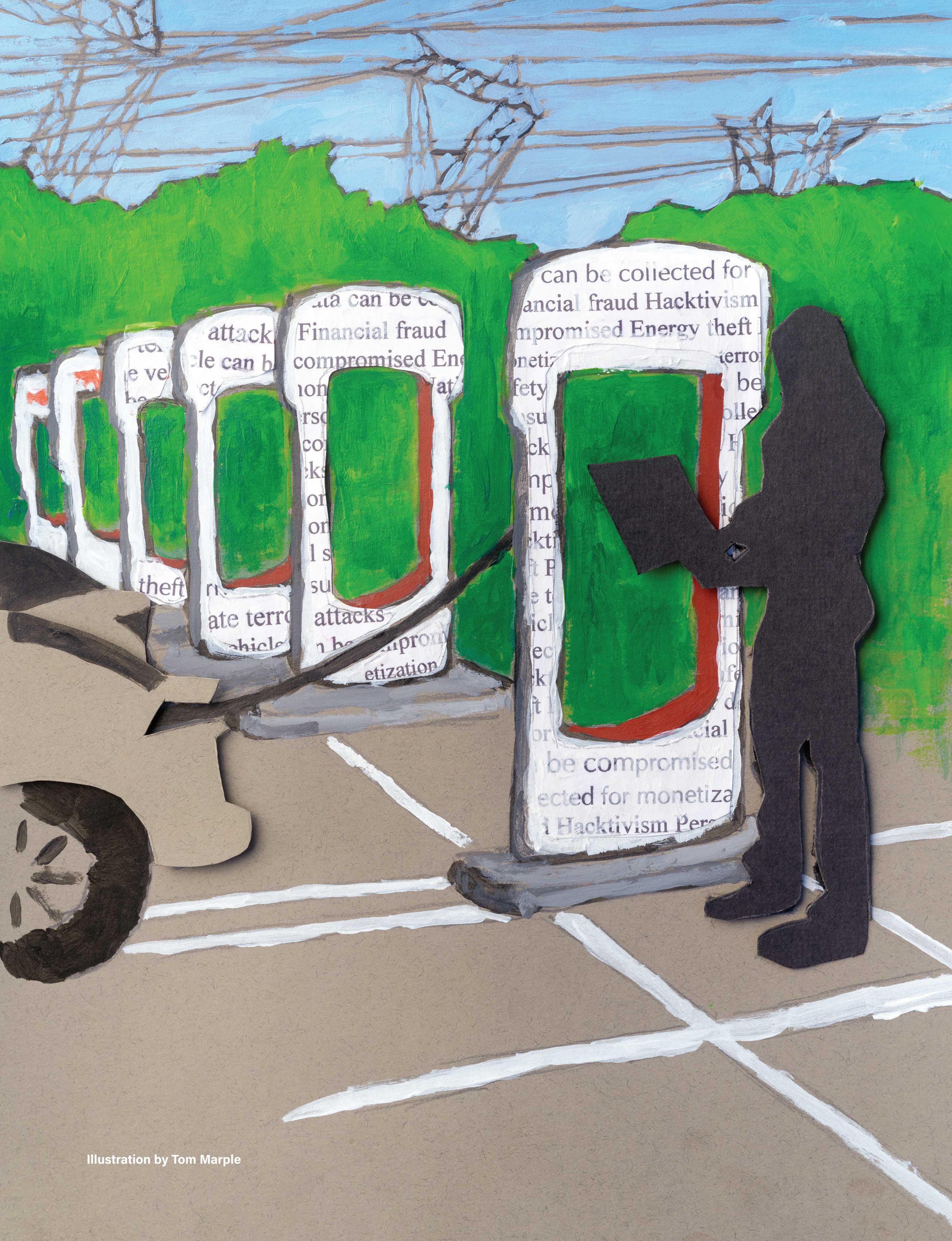


Illustration by Tom Marple

Half a Million EV Charging Stations

Low maintenance, improving battery performance and the perception of eco-friendliness have made EVs an attractive alternative with more demand than can be fulfilled. [iii] This has been further spurred by rising gas prices, which have surged by 116 percent in the U.S. since the beginning of 2021. [iv] Last year, 535,000 EVs were sold in the U.S. and 305,000 in the U.K.[v]

Included in the Bipartisan Infrastructure Law, enacted last fall by Congress as the Infrastructure Investment and Jobs Act, is a $7.5 billion[vi] allocation to build 500,000 charging stations.[vii] The Department of Transportation (DOT) published a toolkit on its website to inform the public and disseminate information about the installation and operation of the new EV infrastructure, including best-practice guidelines for the planning and maintenance of charging infrastructure.[viii] However, the increasing challenges that cybersecurity threats pose, as well as effective precautionary measures, are missing from the toolkit.

In June 2022, DOT and the Department of Energy proposed new standards to increase the convenience and reliability of EV charging infrastructure.[ix] Yet, developing and implementing plans to deal with most cybersecurity threats is left to individual states.

Nation-State Attacks

The transportation sector is one of 16 critical cyber-infrastructures in the U.S., designated by the Cybersecurity & Infrastructure Security Agency as potential targets of nation-state sponsored terror attacks.[x]

In recent years, nation-state attacks have increasingly disrupted American businesses and government agencies. According to the Microsoft Digital Defense Report, Russia is responsible for the bulk of nation-state cyberattacks (58 percent), followed by North Korea (23 percent), Iran (11 percent) and then China (8 percent). Between May 2021 and March 2022, for example, a Chinese state-sponsored hacking group, known as "Hafnium," infiltrated at least six state government departments, culminating in a major exploit of the Microsoft Exchange Server software.[xi] The Exchange Server is a popular software used for providing corporate email services. Exploiting this vulnerability afforded Chinese cyber espionage an entry point into the networks of as many as 30,000 victim organizations, including small businesses, towns, cities, local governments and defense contractors. Predictably, China's Ministry of Foreign Affairs denied any involvement.[xii]

In March 2022, the Federal Bureau of Investigation issued a threat warning for American energy systems and other critical infrastructure, stating that Russian hackers were scanning our energy sector for vulnerabilities, as well as conducting reconnaissance of our military defenses.[xiii]

In recent years, U.S. agencies have been prosecuting hacker groups targeting critical infrastructure. In March 2022, federal prosecutors charged Russian officials involved in hacking campaigns that included the energy sector.[xiv] In another incident, a 36-year-old research institute employee at the Ministry of Defence of the Russian Federation was accused of conspiring to hack an oil and gas refinery system in the U.S. and install what is known as "Triton" malware. Triton can communicate with the controllers that manage petroleum-refining operations and transmit halt commands.

Most significantly, in January 2022, Russia's domestic security agency (at the request of the U.S. government) arrested 14 alleged members of REvil, a hacker group[xv] that American officials say masterminded the Colonial Pipeline attack, which crippled East Coast gas supplies last year.[xvi] Colonial Pipeline supplies gas, diesel and jet fuel, and about 45 percent of all East Coast fuels arrives via this pipeline. In May 2021, hackers gained remote entry to Colonial Pipeline's servers through an abandoned Virtual Private Network (VPN) account whose password was leaked onto the dark web. VPN accounts give employees remote access to company networks, and the accounts must be deactivated as soon as no longer in use.

The hackers planted DarkSide malware,[xvii] a relatively new ransomware used for targeting high-revenue organizations. Ransomware is the term given to malware engineered to block access to a computer system, typically by encrypting or scrambling data stored on that system until a ransom is paid. DarkSide's malware is a particularly nasty strain that executes a double extortion tactic by infecting the network domain controller, spreading to other machines and stealing data before finally encrypting it. About 100 GB of data was exfiltrated from Colonial Pipeline's servers.

All operations of the 5,500-mile pipeline were halted for a week to prevent further spread of the ransomware, wipe the affected machines and recover from the damage. This caused a gas shortage, which lead to panic buying. The company ended up paying a ransomware bribe of about $5 million to retrieve the stolen data.

Ransomware Tsunami

The cost of ransomware attacks on the automotive industry, including Honda,[xviii] Toyota,[xix] Nissan and Renault[xx] increased massively from $6.9 million in 2019 to $20 billion in 2020[xxi] and is expected to top $50 billion by 2023. Russian hackers have even bribed Tesla employees[xxii] with million-dollar payments to plant malware in the company's servers enabling malicious access.

Yoav Levy, CEO of Upstream Security, which provides automotive cybersecurity platforms, reports a rise in attacks on both charging stations and EVs.[xxiii] Dishonest owners can hack into the charging station to avoid paying usage fees. Hackers can lock up charging terminals and prevent EV owners from charging their vehicles until a bribe is paid. Vehicle fleet owners, such as car rental companies, are much more susceptible to such attacks than are charging station homeowners, as preventing the fleet from charging will stall business operations and force the owner to pay a large ransom.

Hacktivism

Hacktivism, a mix of "hacking" and "activism," is increasing due to charging infrastructure vulnerabilities. Early in the Russian occupation of Ukraine, a Ukrainian hacker injected an abusive message about Putin into a charging terminal display on a Russian motorway.[xxiv] A similar incident occurred in the U.K. when hackers displayed pornographic content on charging station display screens.[xxv]

Researchers have demonstrated how easy it is for miscreants to halt an entire fleet of electric ambulances parked at a station from charging using malicious radio signals.[xxvi] Dubbed the Brokenwire technique, the attack involves placing a small off-the-shelf radio transmitter, called a software-defined-radio, within 50 yards of the charging station. Then the charging station is bombarded with constant radio signals causing a denial-of-service condition whereby the station stops charging all cars immediately. The only way to resume the charge is to physically walk up to the charger and unplug it and then resume the charging process.

In April 2022, several charging stations on the Isle of Wight, U.K., were hacked such that inappropriate content from pornographic websites was shown the display screens.[xxvii] The hackers also made the charging stations unavailable: Every time a customer tried to use the station, it rebooted. However, no ransomware demand was reported.

Personal Safety

Personal safety while driving in an EV can be compromised by hackers exploiting onboard vulnerable apps to unlock doors, open windows or flash the headlights.[xxviii] In 2016, a similar attack on the NissanConnect app allowed hackers to control an EV's air conditioning.[xxix] In another instance, hackers exploited a popular car communications app called UConnect, forcing a Jeep to drive into a ditch and caused Chrysler, one of the brands using this app, to recall 1.4 million vehicles.[xxx] Such attacks in future might prove fatal.

Numerous vulnerabilities exist in wireless protocols used in the design of keyless technologies that make EVs, as well as other vehicles with keyless technology, susceptible to car theft. The simple "relay attack" was used in multiple car thefts in South Austin, Texas, in May this year. The attack only requires two inexpensive Bluetooth radios, which the hackers configured to redirect Bluetooth communications normally used by keyless-entry fobs. To execute, the thieves place one of the devices next to the car they are targeting, when parked in the owner's driveway. The other device is placed just outside the front door of the house, presumably near where the owner left the car fob on the other side of the door. Signals emitted by the fob are automatically relayed from one device to the other, creating the impression that the owner is located close to the vehicle, allowing the entry system to be fooled and the thieves to drive off with the car.[xxxi]

The hacking device also works with smartphones. Since the device can pick up signals anywhere within 15 yards of the phone, placing the smartphone outside the bedroom window where the owner's smartphone is charging, for example, will also enable an attack.

Energy Theft

Energy theft will increase with EV use since recharging tightly couples transportation and the power grid. Recent research involving multiple universities analyzed the management software at 16 charging stations by examining the charger firmware, as well as the mobile and web applications customers use to interact with the charger.[xxxii] The authors found several web-server vulnerabilities in the products of several companies. Additionally, they found that by exploiting these vulnerabilities attackers can control the charging processes, modify firmware settings, change the billing, access personally identifiable information and even recruit the system for botnet operations (which use smart devices as a hacking device to attack another device or system). They concluded that hacking operations can also indirectly cause service disruptions and even failure in the local electric grid, which could initiate a cascading effect on the national grid.

EV owners sometimes use their car batteries for crypto mining. One Tesla owner claims to earn $800 in bitcoin every month by rigging his car battery to run mining software.[xxxiii] However, mining for cryptocurrency might void the car's warranty. On the flip side, EV automakers such as Ontario-based Avvenire are adding provisions to allow crypto mining while parked. However, this will shorten the life of the EV battery.[xxxiv]

Cryptojacking private EVs, by hacking the battery to mine cryptocurrency without the owner's knowledge or permission, might soon become a threat. Already cryptojacking attacks have been mounted on the automotive industry. In 2018, hackers infiltrated Tesla's cloud servers through an account that was not properly password protected. They planted cryptojacking malware called Stratum in their Amazon Web Service accounts to mine cryptocurrency using the cloud's computing power.[xxxv]

Private Data

The illegal profits made from car theft, extortion via ransomware or manipulation to lower charging fees pale in comparison to what can be made from stealing EV data. EVs track performance and record the surroundings using sensors and cameras, generating much more data than traditional vehicles. The data can tell us where to park, when an engine part needs replacement, and even how many pedestrians and/or vehicles are on a block. Even when not driving, EVs are still generating data that can be mined for profit, just as Big Tech companies such as Google and Meta make money from free services that enable access to user date.

Today, many companies profit legally by selling vehicle data, for example to identify open parking spaces or provide personalized location-based advertising. McKinsey & Company, a global consulting firm, estimated in 2016 that the worldwide revenue from car-generated data could reach $750 billion by 2030.[xxxvi]

EV data unlocks tremendous potential to improve driving safety, as well as producing municipal (traffic and parking space information) and commercial benefits. Automotive companies collect data to help drivers manage daily tasks with a few clicks or voice commands and, as noted above, make money by analyzing driver patterns and selling the information to advertisers. However, many EVs integrate third-party apps such as Amazon's Alexa, Google Assistant and Apple's Siri to facilitate voice calls and control home security while driving. Although convenient, third-party apps open security backdoors for hackers, providing access to the driver's personal information, as well as data directly associated with the driving experience. Phone contacts can be extracted from connected apps, and credit card details can be obtained through the dashcam. Further, with the help of car data, hackers can profile the driver via the data as a new form of espionage and use it for extortion, stalking or other criminal purposes.[xxxvii]

The new infrastructure law calls for the installation of monitors for alcohol, impaired driving and child alerts. This promises to significantly reduce fatalities caused by drunk drivers, for example, which accounted for 11,654 deaths in 2020.[xxxviii] The monitors could also reduce the number of children dying from vehicular heatstroke, which total 917 since 1998 in the U.S.[xxxix] Even so, privacy advocates fear that this data might be very compromising if the information is inadvertently leaked or hacked.[xl]

Policy Decisions: Way Forward

EVs are a storehouse of private data, collected constantly by a myriad of sensors, which makes EVs vulnerable to cyberattacks.[xli] To counter this, robust online patch management is essential for handling installation errors.[xlii]

Sometimes servicemen or owners download a patch from the dealership website onto a computer, transfer it onto a thumb drive and stick it into a USB dongle port in the car. Making manual software updates[xliii] should be avoided since the updates might be compromised[xliv] or additional malicious files might trigger malware when connected. Further, there should be a proper patch integrity verification mechanism installed in the vehicle that validates the updates before installation.

Also, as shown by the "TBONE" attack on Teslas in 2021, which used a drone to penetrate the EV's control system, automakers should avoid using hardcoded (also termed, embedded) credentials inside the vehicle.[xlv] Such information can easily be retrieved through eavesdropping or by malware infiltrating the system. Credentials should be stored in a configuration file or a database in encrypted form, and policies should be established for enforcing their rotation and ensuring their complexity.

Since 2011, there has been a significant increase in EV charging infrastructure,[xlvi] as EVs gain popularity. During the same period, the number of EVs in the U.S. increased from 16,000 to two million. However, although EVs account for 19 percent of new car sales in Europe in 2021 and 15 percent in Mainland China, they account for only 4 percent in the U.S.[xlvii]

To scale up securely, a mechanism is needed for physical security checks before the issuance of a permit from the federal government to install a charging station, and only compliant hardware should be allowed.[xlviii] Several popular chargers have used cheap motherboards with insecure design, such as the Raspberry Pi, which has limited support for secure booting; signed firmware, which guarantees security; key storage; hardware encryption; USB port locks; and tamper resistance. Further, a mechanism for data security should be clearly articulated in the permit request form.[xlix] Recently, the U.K. approved comprehensive EV legislation that includes security requirements, which will be implemented nationally in December.[l]

Auto insurance providers cover vehicle accidents and personal liability. It would be helpful to consumers to add provision for cyberattacks.[li] Automotive companies should clearly define the classifications of vehicular data, based on sensitivity, to determine the appropriate sharing and processing procedures. Lastly, to help consumers purchase the most appropriate vehicle and to provide a competitive market environment regarding cybersecurity features, it is important to create a system for cybersecurity ratings in vehicle consumer reports.

The automotive industry should define, create and implement a proper mechanism for remote inspection of customers' vehicles to identify malware and other stealth attacks on EVs and the charging infrastructure. Further, clear policies are required to educate users on the methods and safeguards for dealing with ransomware attacks.

As the EV network matures into a large cyber-physical system, there should be no weak links that can hamper the building of the half-million charging stations nationwide.

[i] https://www.researchgate.net/publication/358402319_Brokenwire_Wireless_Disruption_of_CCS_Electric_Vehicle_Charging

[ii] https://www.israel21c.org/cyberattacks-on-cars-increased-225-in-last-three-years/

[iii] https://www.latimes.com/business/story/2022-04-01/high-gas-prices-drive-ev-demand-but-supplies-short

[iv] https://www.eia.gov/dnav/pet/hist/LeafHandler.ashx?n=pet&s=emm_epmr_pte_nus_dpg&f=w

[v] https://insideevs.com/news/565442/uk-plugin-car-sales-january2022

[vi] https://www.washingtontimes.com/news/2022/jun/8/biden-unveils-rules-for-nationwide-network-of-5000/

[vii] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/07/fact-sheet-vice-president-harris-announces-actions-to-accelerate-clean-transit-buses-school-buses-and-trucks/

[viii] https://www.transportation.gov/sites/dot.gov/files/2022-01/Charging-Forward_A-Toolkit-for-Planning-and-Funding-Rural-Electric-Mobility-Infrastructure_Feb2022.pdf

[ix] https://www.cnet.com/roadshow/news/biden-administration-proposed-ev-charging-standards/

[x] https://www.cisa.gov/critical-infrastructure-sectors

[xi] https://www.cnbc.com/2021/03/09/microsoft-exchange-hack-explained.html

[xii] https://www.cnbc.com/2022/03/09/china-state-backed-hackers-compromised-6-us-state-governments-report.html

[xiii] www.reuters.com/world/fbi-says-russian-hackers-scanning-us-energy-systems-pose-current-threat-2022-03-29/

[xiv] https://www.theguardian.com/world/2022/mar/24/us-charges-russian-hackers-cyber-attacks

[xv] https://www.washingtonpost.com/world/2022/01/14/russia-hacker-revil/

[xvi] https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

[xvii] https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html

[xviii] https://techcrunch.com/2020/06/09/honda-ransomware-snake/

[xix] https://www.zdnet.com/article/toyota-australia-confirms-attempted-cyber-attack/

[xx] https://www.thenationalnews.com/business/carmaker-nissan-says-uk-plant-hit-by-ransomware-attack-1.69769

[xxi] https://www.otorio.com/blog/ransomware-the-cyber-attacks-on-the-automotive-industry/

[xxii] https://www.tripwire.com/state-of-security/featured/closer-look-attempted-ransomware-attack-tesla/

[xxiii] https://www.israel21c.org/cyberattacks-on-cars-increased-225-in-last-three-years/

[xxiv] https://www.independent.co.uk/news/world/europe/putin-charging-station-hacked-ukraine-russia-b2026260.html

[xxv] https://www.bbc.com/news/uk-england-hampshire-61006816

[xxvi] https://www.telegraph.co.uk/business/2022/03/29/security-flaws-leaves-electric-cars-risk-cyber-hacks/

[xxvii] www.news18.com/news/buzz/ev-owners-shocked-after-hacked-charging-station-screens-show-pornographic-photos-5070415.html

[xxviii] www.vice.com/en/article/akv7z5/how-a-hacker-controlled-dozens-of-teslas-using-a-flaw-in-third-party-app

[xxix] https://www.theguardian.com/technology/2016/feb/24/hackers-nissan-leaf-heating-access-driving-history

[xxx] https://www.bbc.com/news/technology-33650491

[xxxi] https://fortune.com/2022/05/17/tesla-hacker-shows-how-to-unlock-start-and-drive-off-with-car/

[xxxii] https://www.sciencedirect.com/science/article/pii/S0167404821003357

[xxxiii] https://thehill.com/changing-america/enrichment/education/589045-how-tesla-owners-can-mine-cryptocurrency-with-their/

[xxxiv] https://news.yahoo.com/this-electric-vehicle-mines-crypto-in-its-free-time-191748861.html

[xxxv] https://www.investopedia.com/news/teslas-cloud-was-hacked-mining-cryptocurrency/

[xxxvi] https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/monetizing-car-data

[xxxvii] https://venturebeat.com/2022/05/15/car-hack-attacks-its-about-data-theft-not-demolition/

[xxxviii] https://www.responsibility.org/alcohol-statistics/drunk-driving-statistics/drunk-driving-fatality-statistics/

[xxxix] https://www.noheatstroke.org/

[xl] www.aclu.org/news/privacy-technology/congressional-drunk-driver-detection-mandate-raises-privacy-questions

[xli] https://upstream.auto/blog/the-hidden-cyber-risks-of-electric-vehicles/

[xlii] www.tesla.com/support/software-updates

[xliii] ww.forbes.com/sites/thomasbrewster/2015/01/15/researcher-says-progressive-insurance-dongle-totally-insecure

[xliv] https://securityboulevard.com/2021/03/patch-management-in-the-post-solarwinds-era/

[xlv] https://www.thedrive.com/tech/40438/researchers-used-a-drone-and-a-wifi-dongle-to-break-into-a-tesla

[xlvi] https://afdc.energy.gov/fuels/electricity_infrastructure_trends.html

[xlvii] https://www.canalys.com/newsroom/global-electric-vehicle-market-2021?ctid=2627-70a8050e26f41f72baaf6b38e200993a

[xlviii] https://techcrunch.com/2021/08/03/security-flaws-found-in-popular-ev-chargers/

[xlix] https://afdc.energy.gov/files/pdfs/EV_charging_template.pdf

[l] https://www.gov.uk/government/consultations/electric-vehicle-smart-charging

[li] www.insurancebusinessmag.com/us/news/cyber/electric-vehicle-cybersecurity-business-owners-worried-about-the-risks-398832.aspx

Scene from Steven Spielberg's "Ready Player One" (2018) in which the main character's avatar views a shield dome erected by the movie's villain around a competition in a virtual world.

Trouble in the Metaverse

Whatever That Is?

JEREMY STRAUB, PHD
Assistant Professor of Computer Science, North Dakota State University

Steven Spielberg's 2018 movie, "Ready Player One," portrays a dystopian world in which society has moved mostly online. Three years later, we learned that this imagined cyber environment—hopefully not dystopian—was being built as the 'metaverse,' and that Meta (the company formerly known as Facebook) was positioning itself to be a dominant player in this new market.[i]

Recently, Mark Zuckerberg, the founder of Facebook and Meta, predicted that the metaverse will become a $100 billion plus commercial platform with a billion people spending "hundreds of dollars each" on "digital goods" and digital content, such as "clothing for their avatar," "digital goods for their virtual home" and "things to decorate their virtual conference room."[ii] Individuals are buying up "land" in the metaverse,[iii] retailers are already buying virtual shop space,[iv] and Meta has launched a "designer clothing store for avatars."[v] Meta is also training metaverse workers with newly launched Metaverse Academies in France.[vi] The company hopes to capture a piece of these transactions with its Meta Pay digital wallet system.[vii]

There will, no doubt, be many challenges to establishing a fully functional metaverse. This article serves to facilitate discussion concerning several potential key problems.

What is it?

Perhaps the metaverse's biggest issue is that most people don't even know what it is. An Axios survey found that about two-thirds of respondents "weren't exactly sure" what the metaverse is, and that most were neither excited nor concerned about it.[viii] Former Google CEO Eric Schmidt suggested that the problem is larger than this. At the Aspen Ideas Festival in July, he said that among the people and companies building the metaverse, "there isn't an agreement on what the metaverse is."[ix]

At its most fundamental level, the metaverse is an area for people to live, play and work online. It will likely be enabled by virtual and augmented reality and be an immersive environment, like the online space in "Ready Player One."

According to Meta, "the metaverse will feel like a hybrid of today's online social experiences, sometimes expanded into three dimensions or projected into the physical world. It will let you share immersive experiences with other people even when you can't be together—and do things together you couldn't do in the physical world." [x] What exactly this is, though, is still unclear. Perhaps it could become "the future of the internet," wrote Eric Ravenscraft in Wired magazine, or "a video game" or "a deeply uncomfortable worse version of Zoom," noting that since Meta's announcement "what that term means hasn't gotten any clearer."[xi]

Perhaps the most important question is whether the metaverse will be a single system in which users can easily jump among areas (perhaps called virtual "worlds") using a single interface and login. Right now, numerous online immersive and interactive systems are considered part of the metaverse. However, these have different interfaces, user accounts and hardware support capabilities. Certainly, the current-day metaverse falls short of the online environment in "Ready Player One" in terms of the consistency of user experience. What the future holds remains vague.

Government in the Metaverse

While the question of whether the metaverse is or becomes one environment; a collection of environments; or a name for certain types of competing, and perhaps even incompatible, systems is complex, this is not the most daunting issue. Several broader questions—relating to how society functions in an online environment—demand consideration.

The first is the role of government. While the metaverse is virtual, its servers, payments and users exist in the physical world. The locations of corporations, workers, servers and users create connections to the laws of numerous countries and, within the U.S., state and municipal jurisdictions.

The metaverse will, thus, barring significant political actions, operate subject to a patchwork of legal environments. While big companies, such as Meta, might be able to navigate this complex regulatory environment successfully, smaller businesses—such as those buying up virtual land—might find it far more difficult. System users might also become ensnared in the laws of distant lands. For example, imagine a scenario where a user steals from another player as part of a metaverse role-playing game. While this may be an accepted part of gameplay, because the stolen assets have value—they can be bought and sold—theft in the virtual world could involve lawsuits or criminal prosecutions in the real world. Some liability could be disclaimed via contract: You can't claim that something is stolen, for example, if you agreed to permit theft when you signed the agreement to play the role-playing game. However, this is a complex, multilayered arena upon which considerable focus must be placed.

Another question is access to records. When all actions are online, they can be easily recorded and subject to government review. What would stop governments from using the environment's technology to covertly surveil its citizens in order to facilitate enforcement for even the most minor infractions in the virtual world? Technologically, the answer is very little. For those who worried that Big Brother might follow cars around with drones to issue tickets, the metaverse is the next potential frontier of surveillance-enforcement. Even the most basic right to privacy is challenged when every action and interaction is stored on corporate servers readily accessible to the (perhaps more correctly, every) government. Because of this widespread access, multiple governments might seek to enforce their—potentially conflicting—laws ubiquitously within the online environment, creating legal chaos.

Companies operating in the metaverse will also have to be acutely aware of the physical location of users to avoid violating trade restrictions and tariffs. Government restrictions on online access and interacting with citizens of other nations might

The cold-storage Meta data center houses the immense data storage and computer processing that powers the parts of the metaverse the company is currently building. Image courtesy of Meta.

prevent some users from accessing various online possessions and conducting proscribed transactions. Of course, users may conduct these illegal transactions unwittingly, if metaverse operators don't alert them to users' locations and applicable restrictions, or automatically block them.

In an extreme situation, parts of the metaverse may end up duplicated and operating independently if servers and users in one country or region and those in another are prevented from communicating with each other, and both have an operating copy of a virtual world from before the links were severed. This could cause the duplication or reappropriation of digital assets, in addition to considerable user confusion and a multitude of related issues.

Potential Risk and Reward

Like all new technologies and business frontiers, the metaverse carries significant potential benefits and risks. For companies, a pervasive online environment means access to customers and workers all over the world. Online employment may be particularly valuable to individuals from regions with lower wage levels, who would enjoy substantially higher wages in a global workplace. However, these same forces would tend to lower wages in areas that have typically enjoyed higher income levels.

Other risks include the uncertainty of government regulations, concerns about both corporate and governmental surveillance, and questions regarding the ownership of basically everything (including even digital 'memories') in the online environment. Ensuring the physical health of users, who might become somewhat sedentary while spending huge amounts of time online, is also a major area of concern. Even basic questions regarding who will provide online neighborhood policing and similar services (which typically fall under government jurisdiction) remain unanswered.

The answers to these questions will be key to how (and even if) people live and work in the metaverse. More fundamentally, early regulations and practices will help define the next potential age of human civilization.

[i] https://www.abc.net.au/news/2021-10-29/facebook-rebrands-as-meta-to-harness-virtual-reality-in-future/100578908

[ii] https://www.cnbc.com/2022/06/22/mark-zuckerberg-envisions-1-billion-people-in-the-metaverse.html

[iii] https://futurism.com/the-byte/man-life-savings-metaverse-land

[iv] https://www.bbc.com/news/business-61979150

[v] https://indianexpress.com/article/technology/crypto/meta-announces-digital-designer-clothing-store-for-avatars-in-the-metaverse-7977031/

[vi] https://www.rfi.fr/en/france/20220612-facebook-announces-launch-of-metaverse-academies-across-france

[vii] https://www.theverge.com/2022/6/22/23179058/mark-zuckerberg-meta-pay-wallet-metaverse-details

[viii] https://www.cnbc.com/2022/07/01/ex-google-ceo-eric-schmidt-theres-no-definition-of-the-metaverse-yet.html

[ix] https://www.cnbc.com/2022/07/01/ex-google-ceo-eric-schmidt-theres-no-definition-of-the-metaverse-yet.html

[x] https://about.fb.com/news/2021/10/facebook-company-is-now-meta/

[xi] https://www.wired.com/story/what-is-the-metaverse/

CYBERSECURITY in healthcare needs an **URGENT UPGRADE,** especially since **MEDICAL DEVICES** can be **HACKED** without any indication.

Security Vulnerability in Medical IoT Devices

ALAIN LOUKAKA, PHD, Application Support Consultant

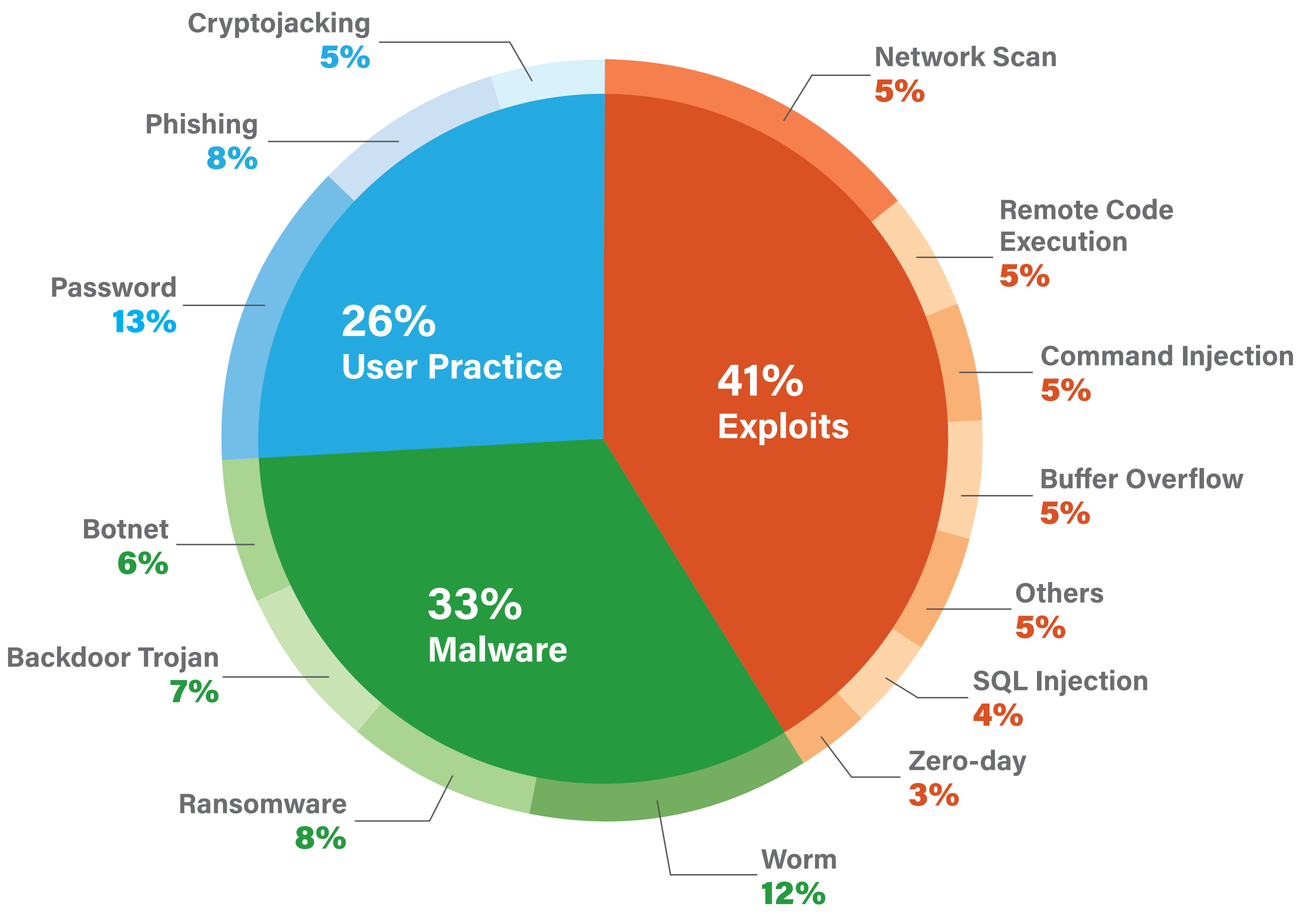
SHAWON RAHMAN, PHD, Professor of Computer Science
University of Hawaii at Hilo

According to the Palo Alto Networks threat report,[i] 98 percent of IoT (Internet of Things) device traffic is unencrypted, exposing personal data on hospital networks. In addition, 72 percent of healthcare Virtual Local Area Networks (VLANs) mix IoT and IT assets, allowing malware to spread from computers to vulnerable IoT devices on the same network. These vulnerabilities allow hackers to access network traffic and collect confidential information, then exploit that data for profit on the Dark Web or alter data to cause harm.

Major cyberattacks, aimed at either disrupting or extorting a system, have always targeted significant entities such as power grids, supervisory control and data acquisition (SCADA) system architecture, and healthcare systems. Manufacturing and healthcare systems are so susceptible that they will suffer 74 percent of all attacks by 2025, according to the Palo Alto report. Also, vendors' and manufacturers' software can be compromised and allow hackers to access devices, such as an insulin drip.[ii]

In recent years, ransomware attacks on hospitals have increased, including the famous WannaCry hack aimed at hospital CCTV cameras. Malicious users block authenticated users from access to their files and hold the data hostage until a ransom is paid. Countermeasures are important to protect system files and promote computer hygiene, such as up-to-date antivirus software, data back-up (preferably on an external or offsite drive), disabling unused ports and applying any security patches for the operating system such as Windows.[iii] Regardless of the attack sources—criminal organizations, nation states or script kiddies—cyberwarfare is tremendously harmful. Exfiltrated patient data can be used for identity theft and other forms of fraud. Stealing confidential patient information contributes significantly to the ongoing rise in identity fraud nationwide.[iv]

Worse, patient information can be altered—or deleted—regarding treatment and drug names and dosages, with potentially catastrophic results. Patients can suffer severe injury or even die if a hacker gains unauthorized access to monitoring or other medical equipment and outputs false data. Similarly, devices administering medicine, such as infusion and insulin pumps, can be shut off or dosages wrongly increased by hackers. Imagine the potential harm if a hospital's power, including backup generators, is turned off. Monitoring screens go blank, or cardiac devices are compromised, or access to the blood supply is blocked during major surgery, such as a double transplant.



In the graph above, non-secure IoT devices account for about half of reported cyber-exploits in all industries.

User online practices represent 26 percent of all threats. Half of these concern password issues, followed by phishing and cryptojacking. Malware accounts for a third of threats, shared by worm attacks at 12 percent and almost equally by ransomware, backdoor trojans and botnets at 6, 7 and 8 percent, respectively. The largest proportion of threats involve exploits at 41 percent, with network scans at 14 percent; remote code execution, command injection, buffer overflow and miscellaneous attacks at 5 percent each; SQL injection at 4 percent; and Zero-Day attacks at 3 percent.

Based on the report, when security measures such as patches, updates, password and asset management policies are continuously implemented, user-level threats would decrease from 26 to 13 percent, malware threats from 33 to 13 percent, and exploits from 41 to 27 percent.

Cybersecurity in healthcare needs an urgent upgrade, especially since medical devices can be hacked without any indication. Information protection should not become important only after a data breach but throughout the security design that houses both highly secured connections and IoT devices, which are not highly secured connections. When organizations fail to upgrade security due to budget restraints, they might have to pay a hefty ransom to have the malware flushed out of their systems and their data released.

Vulnerability

Ransomware attacks have increased tremendously since their first detection in 1989.[v] The cost of ransomware attacks has skyrocketed from $10 to $210 billion from 2015 to 2021, which illustrates the importance of securing IoT devices.[vi] Examples of ransomware targets in 2021 include Kaseya, an IT management and security software company, ($70 million in Bitcoin),[vii] and JBS USA Holdings, Inc., a food processing company, ($11 million in Bitcoin).[viii]

Both Kaseya and JBS were hacked by REvil, a Russian cybercriminal organization, which attacked more than 360 American targets in 2021. REvil then leveraged Kaseya's "connectivity to the larger internet ecosystem to infect more than 1,500 organizations around the world."[ix]

Among the major areas where IoT devices are primarily targeted, the healthcare industry leads the way at 41 percent of attacks, as shown in the graph below, because of the ease with which medical devices can be penetrated.[x] The tremendous growth of the internet has made device accessibility more prolific. Imaging devices alone account for 51 percent of threats to healthcare organizations. As a result, there have been many high-profile breaches that amplified the need for robust cybersecurity measures to combat ransomware attacks.

Malicious network and Denial of Service (DoS) attacks are the most dangerous. Today's doctors and nurses must stay connected to various medical devices in real-time since these machines are integral to diagnosis and treatment.[xii] An additional area of concern involves vendors and manufacturers whose software can be compromised, which might allow hackers access to medical devices.[xiii]

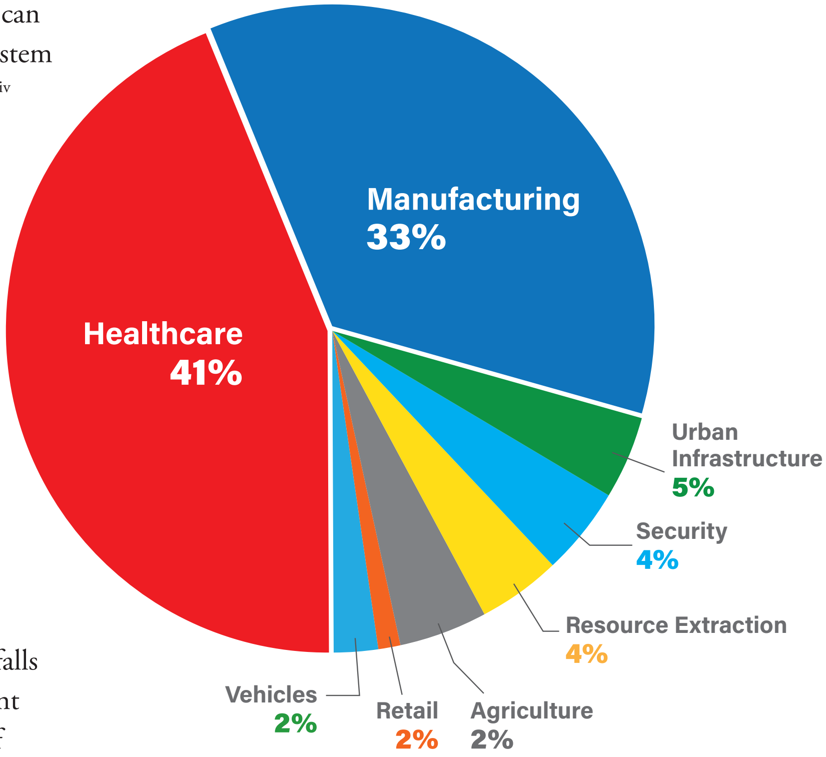
The graphic on page 56 shows how hackers can perform various malicious attacks on any system without security improvements or updates.[xiv] Because the statistics show more than 50 percent probability of exploit success, it is a matter of time before half of the healthcare systems are hacked from outside threats, especially from Zero-Day attacks that, since new, are difficult to detect by intrusion and prevention systems (IDPS).[xv] Fortunately, based on the Palo Alto report, these account for only 3 percent of exploits.

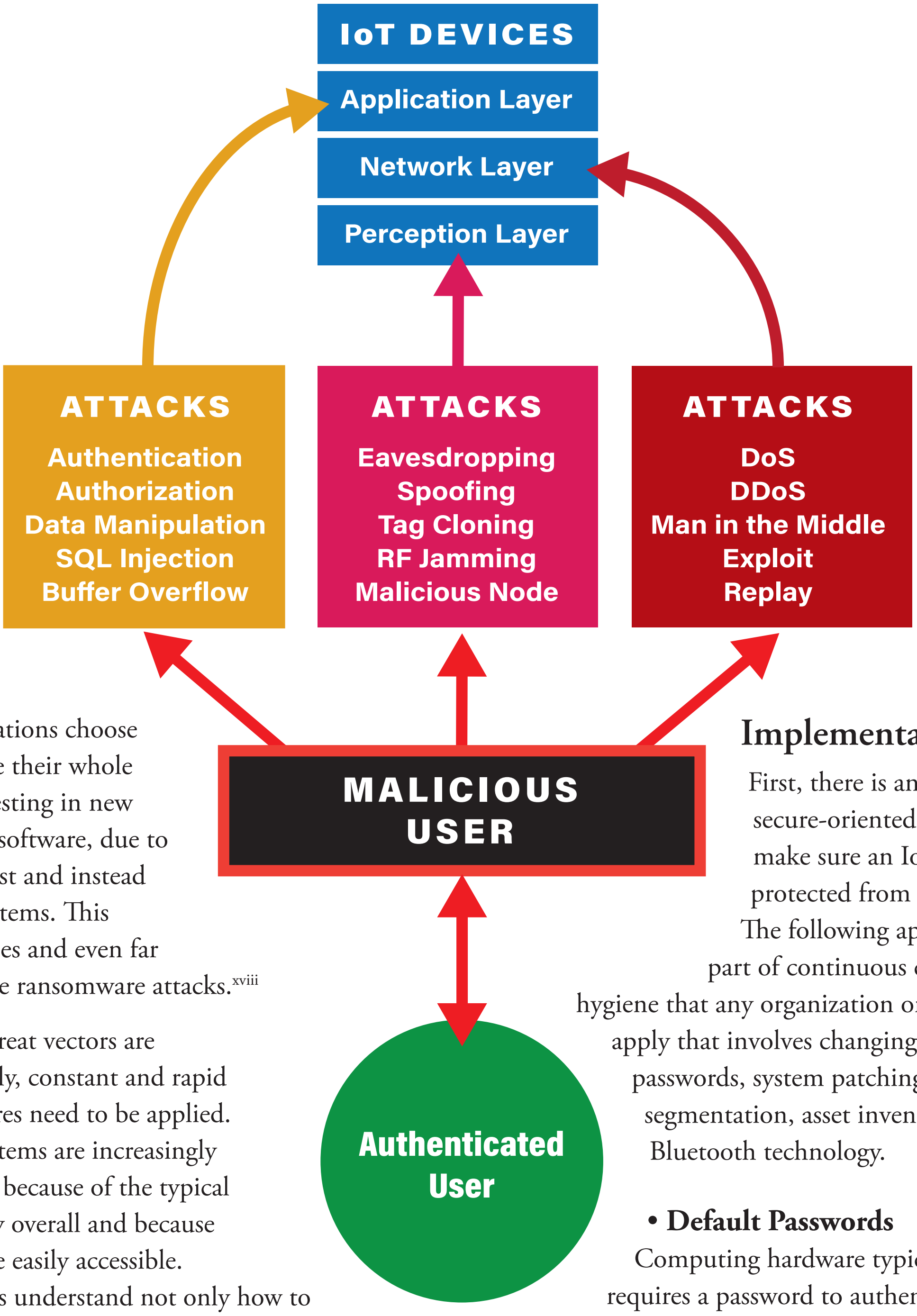
Prevention

It is imperative to focus on security from a defensive perspective before an IoT system falls for ransomware. Security measures to prevent unauthorized access must use a high level of encryption, server backups, access controls, virus scanners, and up-to-date security software and updates. Data security is always a concern regardless of the type of industry in which the data is located.[xvi]

Cybersecurity is a continuous process in which vendors and consumers must work unequivocally in sync. At this point, most healthcare centers appear to provide adequate security, but it's impossible to verify since many if not most intrusions are never reported, due to the potential negative economic and reputational damage.

Encryption is critical, along with routine updates and constant research to understand the attack surface and help develop better-secured devices. A robust authentication algorithm will make it harder to access a device maliciously.[xvii] The Health Insurance Portability and Accountability Act (HIPAA) is responsible for the federal protection of individual healthcare data, while the National Institute of Standards and Technology (NIST) is the agency that promotes American innovation in technology to provide suitable security measures and guidelines to organizations, but more investment is needed to prevent data leaks and cyberattacks.





Many organizations choose not to upgrade their whole system by investing in new hardware and software, due to the massive cost and instead patch their systems. This enables breaches and even far more expensive ransomware attacks.[xviii]

Since cyber-threat vectors are growing quickly, constant and rapid countermeasures need to be applied. Healthcare systems are increasingly being targeted because of the typical lack of security overall and because IoT devices are easily accessible. Cybercriminals understand not only how to exploit systems but also how to remain undetected for months after a breach.[xix] Outsider attacks, however, are not as successful as insider attacks.[xx] The configuration of internal systems is vital, therefore, and any error can become costly. Also, disgruntled employees might leave themselves backdoor access to extract or upload a virus to disrupt daily business needs. The security apparatus must be appropriately configured to target such specific threats. Individual health information is federally mandated to be protected, and medical facilities must understand the risk of using IoT devices without proper cybersecurity.[xxi] [xxii] [xxiii]

Implementation

First, there is an important secure-oriented approach to make sure an IoT system is protected from cyber harm. The following approach is part of continuous computer hygiene that any organization or user can apply that involves changing default passwords, system patching, network segmentation, asset inventory and Bluetooth technology.

- **Default Passwords**

Computing hardware typically requires a password to authenticate. When a default password is provided, it needs to be changed by the user. Much stolen data is available on the Dark Web, a collection of internet sites accessible with a specialized browser, where users can buy and exchange stolen data. Good password hygiene must be alpha numeric with at least one special character and an uppercase. Also, the password must be changed every 60 to 90 days to prevent brute force attacks, which hackers use to discover passwords in plain text.

- **Unpatched Systems**
  As with passwords, unpatched systems are a prime target for hackers and the main reason for the increased ransomware attacks. A patch management policy must automate security updates, as in Microsoft software, so that hardware and software are up to date, especially on critical systems.
- **Network Segmentation**
  Network segmentation is imperative to limit malicious users from progressing from creating a breach to moving easily within the network and altering or stealing data. IoT devices must be located on a different system segment to be isolated from direct unauthorized access.
- **Asset Inventory**
  Maintaining an active inventory of network-approved devices can facilitate patch implement when attacked, such that bad actors cannot use authorized or unauthorized devices to deploy malware and learn the system's configuration or analyze data traffic.
- **Bluetooth Connection**
  Bluetooth is the go-to method for IoT devices to connect to a network. However, Bluetooth is susceptible to a man-in-the-middle attack in which an attacker gets in between a user and the application—for example, by providing a free but malicious public WIFI hotspot—to eavesdrop or steal or alter the communication or data. Turning off the discoverable option when paired with a device is recommended so no malicious user can detect the connection since it's invisible. Also, malicious hotspots typically aren't password protected.

Second, integrity ensures that the data is not being altered by unauthorized users.[xxiv] [xxv] The mechanism also implemented for data confidentiality (protection against unauthorized access) can also benefit data integrity. Since the data cannot be viewed or deciphered, it cannot be altered in any way. It is equally essential to maintain such a system for access controls, data validation, audit trail, and, most importantly, data backup in case of total loss or inaccessibility as with a ransomware attack.

One proposed solution would be to enhance data security using a blockchain approach.[xxvi] Essentially, blockchain is information recorded in blocks that are highly difficult to breach, modify or access.[xxvii] This technique is used with transactions of Bitcoins and other cryptocurrencies to protect transactions and their anonymity. Using blockchain with IoT devices would provide robust security and reduce organizational costs in rebuilding the database and exploited network post-attack.

Last, availability ensures that data can always be accessed flawlessly without interruption.[xxviii] This is critical to using IoT devices in healthcare, since availability enables uninterrupted, real-time access to patient data for the proper diagnosis and monitoring. Ensuring availability requires investments in reliable data storage systems, secure Wi-Fi, an air-gapped network (which has no interface, wired or wireless, with outside networks) and the latest mobile technology operated properly. Also, critical areas of hospitals must be secured with a keypad access card, security officers and surveillance cameras.

The budget to implement a more efficient network system, especially if significant upgrading is required, might be expensive and time-consuming—but essential to security. Then once accomplished, the system's implementation, maintenance and configuration must be constantly improved.

IoT devices are a growing technology that is becoming ubiquitous. Security concerns need to be addressed immediately to strengthen data integrity and availability.[ixxx] [xxx]

Banks, which protect people's money, have far better security in place than the healthcare sector, which is required to protect people's personal information, as well as their health and lives. It's time for health to pay attention to wealth. ▣

[i] Palo Alto Networks, "2020 Unit 42 IoT Threat Report," https://unit42.paloaltonetworks.com/iot-threat-report-2020/

[ii] Joyia, G. J., Liaqat, R. M., Farooq, A., & Rehman, S. (2017). "Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain." J. Commun., 12(4), 240-247. July 7

[iii] Zou, Y., Roundy, K., Tamersoy, A., Shintre, S., Roturier, J., & Schaub, F. (2020, April), "Examining the adoption and abandonment of security, privacy, and identity theft protection practices," *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems,* (pp. 1-15).

[iv] Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). "Internet of things and ransomware: Evolution, mitigation and prevention," Egyptian Informatics Journal, 22(1), 105-117.

[v] Leo, P., Isik, Ö., & Muhly, F. (2022). "The Ransomware Dilemma," MIT Sloan Management Review, 63(4), 13-15.

[vi] Keary, J. (2022), "Rebuffing Russian Ransomware: How the United States Should Use the Colonial Pipeline and JBS USA Hackings as a Defense Guide for Ransomware," Seton Hall University Law Library, 2022.

[vii] Mohurle, S., & Patil, M. (2017), "A brief study of wannacry threat: Ransomware attack 2017," International Journal of Advanced Research in Computer Science, 8(5), 1938-1940.

[viii] Bunge, J., "JBS Paid $11 Million to Resolve Ransomware Attack," Wall Street Journal, June 9, 2021.

[ix] Collier, K., "Major Russian-speaking ransomware gag behind JBS and Kaseya attacks goes offline," NBC News, https://www.nbcnews.com/tech/tech-news/russian-speaking-ransomware-gang-goes-offline-rcna1403.

[x] Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017), "The rise of ransomware and emerging security challenges in the Internet of Things," Computer Networks, 129, 444-458.

[xi] Djenna, A., Harous, S., & Saidouni, D. E. (2021). "Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure." Applied Sciences, 11(10), 4580. doi:http://dx.doi.org/10.3390/app11104580.

[xii] Hassija, V., Chamola, V., Bajpai, B. C., & Zeadally, S. (2021). "Security issues in implantable medic al devices: Fact or fiction?" Sustainable Cities and Society, 66, 102552

[xiii] Joyia, G. J., Liaqat, R. M., Farooq, A., & Rehman, S. (2017). "Internet of medical things (IoMT): Applications, benefits and future challenges in healthcare domain." J. Commun., 12(4), 240-247.

[xiv] Chacko, A., & Hayajneh, T. (2018). "Security and privacy issues with IoT in healthcare." EAI Endorsed Transactions on Pervasive Health and Technology, 4(14) doi:http://dx.doi.org/10.4108/eai.13-7-2018.155079.

[xv] McGowan, A., Sittig, S., & Andel, T. (2021). "Medical Internet of Things: A Survey of the Current Threat and Vulnerability Landscape." In Proceedings of the 54th Hawaii International Conference on System Sciences (p. 3850).

[xvi] Somasundaram, R., & Thirugnanam, M. (2021). "Review of security challenges in healthcare internet of things." Wireless Networks, 27(8), 5503-5509.

[xvii] Kolokotronis, N., & Shiaeles, S. (Eds.). (2021). *Cyber-Security Threats, Actors, and Dynamic Mitigation,* CRC Press (2021).

[xviii] Loukaka, A., & Rahman, S. (2017). "Discovering new cyber protection approaches from a security professional prospective." International Journal of Computer Networks & Communications (IJCNC) Vol, 9.

[ixx] Shepherd, A., Kesa, C., & Cooper, J. (2020). "Internet of Things (IOT) Medical Security: Taxonomy and Perception." Issues in Information Systems, 21(3).

[xx] Chanal, P. M., & Kakkasageri, M. S. (2021). "Preserving Data Confidentiality in Internet of Things." SN Computer Science, 2(1), 1-12.

[xxi] Nadikattu, R. R. (2020). "Data Safety and Integrity Issue in IoT." International Journal for Research in Applied Science & Engineering Technology (IJRASET), 8(VI).

[xxii] Mishra, B., & Padhy, N. (2021). "Enhancing the security, reliability, and data integrity issues in the internet of things by implementing blockchain strategy in mining: challenges and solutions." In Communication Software and Networks (pp. 137-144). Springer, Singapore.

[xxiii] Atlam, H. F., Azad, M. A., Alzahrani, A. G., & Wills, G. (2020). "A Review of Blockchain in Internet of Things and AI." Big Data and Cognitive Computing, 4(4), 28.

[xxiv] Tang, S., & Xie, Y. (2021). "Availability Modeling and Performance Improving of a Healthcare Internet of Things (IoT) System." IoT, 2(2), 310-325.

[xxv] Singh, R. P., Javaid, M., Haleem, A., & Suman, R. (2020). "Internet of things (IoT) applications to fight against COVID-19 pandemic." Diabetes & Metabolic Syndrome: Clinical Research & Reviews, 14(4), 521-524.

[xxvi] Stiawan, D., Suryani, M. E., Idris, M. Y., Aldalaien, M. N., Alsharif, N., & Budiarto, R. (2021). "Ping Flood Attack Pattern Recognition Using a K- Means algorithm in an Internet of Things (IoT) Network." IEEE Access, 9, 116475-116484.

[xxvii] Shah, Y., & Sengupta, S. (2020, October). "A survey on Classification of Cyber-attacks on IoT and IIoT devices." In 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0406-0413). IEEE.

[xxviii] Fernandez, E. B. (2020). "A pattern for a Secure Cloud-Based IoT Architecture." In Proceedings of the 27th Conference on Pattern Languages of Programs (PLOP"20). Association for Computing Machinery, USA.

[xxix] Best, J. (2020). "Could implanted medical devices be hacked?" BMJ, 368.

[xxx] Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., & Dobalian, A. (2020). "Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations." Journal of Medical Systems, 44(5), 1-9.

OPINION

Whangdepootenawah!?

Technological Disruption & Demographic Collapse ~Part One~

PATRICK J. MCCLOSKEY
Editor, Dakota Digital Review

Cola vera ver el final de la crisis **(The queue to see the end of the crisis). Illustration by Jaime Lluch: www.flickr.com/photos/elsilencio/**

In Ireland in the 1840s, a potato blight precipitated famine during which millions of Irish emigrated to the Americas or starved to death. Centuries earlier, the English took control of the Emerald Isle, and the official policy towards impoverished Irish peasants was, in the phraseology of Klaus Schwab, PhD, founder and executive chairman of the World Economic Forum: "You will own nothing, and we don't care if you are happy."

By the turn of the 19th century, the Irish population had increased far beyond what landowners needed to run their farms and plantations. The poor were increasingly regarded as a 'useless class' and financial burden. When the potato blight hit, there was plenty of food grown on Ireland's ecstatically green fields, but it was exported to England.

What to do about the starving Irish masses? 'You will *be* nothing' was the elite's verdict, and emaciated corpses of entire families littered roadways through lush pastures.

That was the Old Green Deal, and perhaps we are in for a technologically driven redo on a global scale. According to Yuval Noah Harari, author of *Homo Deus: A Brief History of Tomorrow* (2016), digital and other advanced technologies will soon produce a vast new useless class. At the same time, world leaders are aggressively pushing the New Green Deal, which threatens to impoverish, oppress and starve millions worldwide.

A true *whangdepootenawah*, defined as an Ojibwe word for "disaster" in the humorously satirical *Devil's Dictionary*—but not in any online Ojibwe dictionaries. Perhaps a made-up word is most appropriate for a man-made catastrophe.

Demographic Winter Is Coming

At first glance, we still seem to be doing alright, despite current economic woes. There are ubiquitous worker shortages—not so useless, yet. But futurists tell a different, paradoxical story. On the one hand, impending demographic collapse would seem to make people more valuable to society. On the other hand, the automation/artificial intelligence (AI) revolution threatens to make most humans superfluous.

"Today the majority of the industrial nations are heading toward demographic death," wrote David P. Goldman in *It's Not the End of the World; It's Just the End of You: The Great Extinction of Nations*, published in 2011. "For the first and only time in recorded history … prosperous, secure and peaceful societies facing no external threat have elected to pass out of existence." (pg. 15)

Since then, the crisis has grown worse, as documented by Peter Zeihan in *The End of the World is Just the Beginning: Mapping the Collapse of Globalization*. Maintaining a country's population requires a 2.1 total fertility rate, which the U.N. calculates "by summing age-specific birth rates over all reproductive ages," typically 15 to 49 years old.

China, the most populous nation with 1.4 billion citizens, has one of the lowest rates at 1.3 and will see its population fall to half by midcentury, wrote Zeihan, an acclaimed geopolitical strategist. At the same time, China also has the fastest aging population in history. There will be many more retired workers, with experience and training—most of whom needing to be supported—than young people entering the workforce. What this means is that China's days as a rising world power are numbered, Zeihan argued, which makes China quite dangerous in the near future.

The same demographic story repeats in the coming decades worldwide and dwarfs all other disruptions. "[C]ountries as varied as China, Russia, Japan, Germany, Italy, South Korea, Ukraine, Canada, Malaysia, Taiwan, Romania … will see their worker cadres pass into mass retirement in the 2020s. None have sufficient young people to regenerate their populations. All suffer from terminal demographics. The real question is how and how soon do their societies crack apart? And do they deflate in silence or lash out?" (pg. 60)

One of the major reasons Russia launched its invasion of the Ukraine this year, Zeihan contended, was because demographics will soon make it impossible to field a large enough force for foreign aggression while simultaneously defending its immense landmass.

Demographic disintegration will repeat in the 2030s and 2040s for nations including Brazil, Spain, Thailand, Poland, Australia and Switzerland. Then in the 2050s, countries including Bangladesh, India, Indonesia, Mexico and Saudi Arabia will face the same fate unless they quickly deal with the crisis.

"The next batch of countries—mostly in the poorer parts of Latin America or sub-Saharan Africa or the Middle East—are even more concerning," (pg. 61) Zeihan continued. Although their populations are far younger, their economies are extractive, importing food and other goods in exchange for exporting raw commodities.

In a globalized world, this model can't make these countries wealthy but does enable survival. However, demographic collapse will precipitate deglobalization, producing massive famine and political upheavals while globalization's jewels—"economic development, quality of life, longevity, health"—will fracture. (pg. 61)

The Weakness of Nations

Ironically, Zeihan cited rapid demographic expansion among globalization's historical gems. Before World War II, various empires competed for raw materials and other resources, which led to armed conflicts. After WWII, the Cold War began and, to contain the Soviet Union, the U.S. instituted a global system of free trade. The U.S. Navy guaranteed security on the high seas, including oil exporting routes from the Middle East, such that any friendly nation could trade with any other friendly nation. This created globalism as we know it and enabled industrialization (or re-industrialization in Western Europe) and massive economic growth around the world.

Industrialization pushed most populations into urban centers as technology made agriculture more productive and less labor-intensive. At the same time, massive amounts of infrastructure and industrial plants needed to be built and then factories run. Jobs and higher standards of living attracted families but also diminished family size. In the countryside, there is room for children and they provide free labor. In the city, kids are very expensive projects. No surprise that birth rates dropped precipitously.

Paradoxically, populations increased dramatically under American-led globalization. The world has been at relative peace, limiting the number of soldiers and civilians killed in conflicts. Technological advances dramatically decreased infant mortality and increased life expectancy. The doubling of China's population over the past 40 years was due mainly to increased life expectancy.

In addition, urbanization offered women paying work outside the home and engendered the women's rights movement, which embraced contraception and abortion. As women filled secondary schools and then universities, the competition between career and family pushed fertility rates below sustainable levels.

The average fertility rate for the European Union is 1.5 and as low as 1.23 in Spain, while South Korea has the lowest at 1.08. Most countries cannot regain replacement birth rates perhaps ever, since economic, societal and military woes, which are interdependent, foretell geopolitical chaos furthering the weakness of nations.

Compound Disinterest

Given the dire nature of demographic collapse and years of forewarning, why have world leaders ignored the problem? Partly, it's not as urgent for Americans. Our fertility rate has declined to 1.78, which gives us a generation to recover, if we start soon.

Even though American media is the least trusted on the planet, according to a recent Reuters Institute survey, it has the biggest megaphone along with social media. Positive stories about increasing family size run counter to the corporate mainstream media's worldview. Nor do the unconceived have advocacy groups.

Also, America is stepping back from protecting global shipping lanes and functioning as the planetary police force. At the same time, regional powers are rising, including Russia, China, India, Turkey, accelerating deglobalization and our detachment from international affairs.

What will result geopolitically is unclear. While China is extending its military reach, Zeihan held that depopulation and deglobalization will cause the nation's breakup. At the same time, China is racing to gain AI superiority, which would render a game-changing advantage. Yet zeroes and ones can neither be eaten nor converted into energy, and China is far from self-sufficient in these. Meanwhile, the U.S. is vying for AI supremacy *and* will have more people of working age than China by 2045. Does population matter?

Displacement & Death by Algorithm

Today we also face a profound technological disruption that, according to Harari, could become devastating for most people. "As algorithms push humans out of the job market," he wrote in *Homo Deus*, "wealth and power might become concentrated in the hands of the tiny elite that owns the all-powerful algorithms, creating unprecedented levels of social and political inequality." (pg. 376)

Worse, this elite in the not-so-distant future will consist of upgraded humans who, due to biotechnical enhancement along with access to the most powerful AI, will "enjoy unheard-of abilities and unprecedented creativity, which will allow them to go on making many of the most important decisions in the world. … However, most humans will not be upgraded and will consequently become an inferior caste dominated by both computer algorithms and the new superhumans." (pg. 403)

Would that Harari was a Hollywood scriptwriter, but he has a PhD in History from the University of Oxford and lectures at the Hebrew University of Jerusalem. His books have sold more than 40 million copies in 65 languages. Recognized as a leading public intellectual, Harari often discusses global challenges with heads of state privately and publicly. In 2018 and 2020, he gave keynote speeches about humanity's future in Davos, where the World Economic Forum annually convenes heads of state, CEOs of 1,000 major corporations and other leaders to decide our future.

Harari also wrote that from the elite's perspective, populations will not only lose their economic utility but their military value too. Vast numbers of unmanned weapons systems (UAS) on land, sea, air and space will replace the massive armed forces of previous eras. Swarms of drones will be deployed more than waves of infantry, "along with small numbers of highly trained solders" and fewer "super-warriors." (pg. 359)

Full robotic autonomy—where UAS would make kill decisions on the battlefield without human control—illustrates the descent of the status of man. This would be "death by algorithm" executed by a sophisticated toaster, as USAF Maj. Gen. (Ret.) Robert Latiff and I wrote in "With Drone Warfare, America Approaches the Robo-Rubicon" in The Wall Street Journal (March 2013).

The Great Decoupling

The underlying technological thrust Harari described as: "Intelligence is decoupling from consciousness." (pg. 361) Until this high-tech moment, tasks requiring intelligence could only be accomplished with humans in charge. He gives examples—playing chess, diagnosing diseases, driving cars—that can now be completed via algorithmic machine learning. Going forward, more tasks and entire professions, including white collar, will be done better, faster and cheaper by computer systems, robots, 3D printing and so on.

Some futurists contend that this technological revolution will create more new occupations than it eliminates. Perhaps, if dynamic free-market capitalism continues to flourish. Even so, in Harari's view, permanent job losses will occur as AI dominates tasks and professions involving cognitive skills.

Yet, some humans will maintain relevancy. Eric Schmidt, Google's former CEO, in interviews after the publication of *The Age of AI and Our Human Future* (2021)*,* which he cowrote with Henry Kissinger and Daniel Huttenlocher, foresaw the ubiquitous presence of AI assistants. While AI is far better than people at pattern recognition and processing data, it is also imprecise and inscrutable. AI can't explain how it arrived at, for example, a disease treatment protocol. Experienced physicians will still be crucial in healthcare, albeit fewer in number.

What is both magnificent and terrifying about AI is its ability to learn and, with increasing computing power, to learn ever more rapidly and intelligently. AI is already being used to compose symphonies and produce paintings. "To make sense of our place in the world," wrote the authors of *The Age of AI and Our Human Future,* "our emphasis may need to shift from the centrality of human reason to the centrality of human dignity and autonomy." (pg. 194)

'What is a human being worth?' is the overwhelming question of this century.

Here's a famous poem by Basho, a 17th-century Japanese haiku master: *The pond is so old, a frog jumps into the sound of water.* If intelligent machines solve urgent complex problems, we cheer. But if an AI program spits out breathtaking verse—or any artistic masterpiece—are we not diving into a mockery of the human soul? We earn wisdom in the painful, irreplaceable struggle to become (the original meaning of the verb "worth"). Become what? A human, who is ever the questioning, the questioner and the question, which is our endlessly reverberating response to Being, whatever that is. No, AI, don't tell us.

Cyber River, Geopolitical Oceans

"[A]ll people in the world are living alongside the same cyber river, and no single nation can regulate this river by itself," Harari said in a TEDx talk in 2017. "All the major problems of the world today are global in essence, and they cannot be solved unless through some kind of global cooperation."

Harari argued that nationalism lacks the scale and scope to resolve these problems. Yes, greater international cooperation is required regarding the myriad of emerging technologies. But as we saw during the recent pandemic, governments throughout the West simultaneously implemented exactly the same repressive and immensely damaging measures (which digital tools enabled but didn't cause). This was less cooperation than lockstep globalism inspired, if not directed, by the World Economic Forum, which trains many world leaders.

The pandemic response was the first stage in realizing the World Economic Forum's vision of the "Great Reset." The vastly more transformative stage, underway already, is the full-scale implementation of iterations of the New Green Deal. The main measures include a forced transition from fossil to green energy sources; blocking fossil fuel development even in poor countries, condemning them to misery; and restricting agricultural production—just as the U.N. warns of multiple famines this year and more in 2023.

Will versions of the New Green Deal produce a *whangdepootenawah* for "useless" humans? Such questions will be discussed in the spring issue of Dakota Digital Review—just as the folly of green energy policies, in eschewing the primacy of abundant food and cheap, reliable fuel, will become blazingly apparent in Europe and elsewhere. Also, to be examined is the underlying rationale that great sacrifices are required to fend off climate change's existential threats, which human activity is allegedly causing. Are climate-emergency claims valid, or do they function as cover for the real objective: a highly technocratic, totalitarian ruling class? Perhaps demographic collapse is seen as an opportunity.

The Great Reset also entails greatly strengthening, via AI, digital methods to censor dissent throughout social media and the internet. "We should … fear AI because it will probably always obey its human masters, never rebel," Harari warned in "Why Technology Favors Tyranny" in Atlantic Monthly (October 2018). "[AI] will almost certainly allow the already powerful to consolidate their power further" potentially creating "a digital dictatorship" in which most "humans risk becoming similar to domesticated animals."

La mujer que me dio la luz. 90 annos **(The 90-year-old women who gave birth to me). Illustration by Jaime Lluch: www.flickr.com/photos/elsilencio/.**

Yet, "[t]oday, a new epoch beckons," the authors of *The Age of AI and Our Human Future* concluded. "Individuals and societies that enlist AI as a partner to amplify skills or pursue ideas may be capable of feats—scientific, medical, military, political and social—that eclipse those of preceding periods." (pg. 205) Solar or lunar?

In Horace, a rural peasant leaves his village and for the first time encounters a river. He sits down to wait patiently for it to flow by. Two millennia later, that river—now cyber— still flows into churning geopolitical oceans driven by deep technological currents. ◘

CONTRIBUTORS

Jerry Anderson serves as the Art Director for Dakota Digital Review. He earned a BA at NDSU and a BS in Design from Minnesota State University Moorhead. He worked for 31 years at the University of Mary as a graphic designer, photographer and instructor in photography. Anderson has published photos in many publications, including many regional newspapers and magazines, the New York Times, US News & World Report and Newsweek. He has also published photos in numerous books, including *Every Place with a Name* (State Historical Society of North Dakota, 1976) and *North Dakota 24/7* (Penguin Random House, 2003).

Zahid Anwar, PhD, serves as Associate Professor of Cybersecurity in the Department of Computer Science and a scholar at the Challey Institute for Global Innovation and Growth at NDSU. He earned an MS and PhD in Computer Science at the University of Illinois at Urbana-Champaign, and he conducted postgraduate research at Concordia University. Previously, Prof. Anwar served on the faculties of the National University of Sciences and Technology in Pakistan, the University of North Carolina at Charlotte and Fontbonne University. He has also worked as a software engineer at IBM, Intel, Motorola, the National Center for Supercomputing Applications, xFlow Research and at CERN on various projects related to information security and data analytics. Prof. Anwar's research focuses on cybersecurity policy and innovative cyber defense. He is a CompTIA certified penetration tester, security+ professional and an AWS certified cloud solutions architect.

The Honorable Kevin Cramer was elected to the U.S. Senate on November 6, 2018 after serving three terms as North Dakota's At-Large Member of the U.S. House of Representatives. He is the first Republican to hold this Senate seat in his lifetime. He serves on the Armed Services, Environment and Public Works, Veterans Affairs, Banking, Housing and Urban Affairs and Budget Committees. Cramer served on the North Dakota Public Service Commission from 2003 to 2012. During this time, he helped oversee the most dynamic economy in the nation. He worked to ensure North Dakotans enjoy some of the lowest utility rates in the United States, enhancing their competitive position in the global marketplace. Cramer earned a BA from Concordia College and a Master's in Management from the University of Mary. On May 4, 2013, Cramer was conferred the degree of Doctor of Leadership, *honoris causa,* by the University of Mary.

Nikola Datzov is an Assistant Professor at the UND's School of Law, where he teaches courses on intellectual property, torts, remedies and conflict of laws. His research and scholarship focus on patent law, artificial intelligence, innovation and the intersection of different areas of intellectual property law. Prior to joining academia, Prof. Datzov was a partner at a large law firm in the Midwest, leveraging his law and computer science degrees in representing parties in high-stakes litigation in federal courts throughout the country. After graduating from law school, Prof. Datzov worked as an attorney in the federal courts for three years, serving as a law clerk for judges at the U.S. Court of Appeals for the Eighth Circuit and the U.S. District Court for the District of Minnesota.

Marcus Fries, PhD, is an Associate Professor and Chair of the Department of Mathematics and Computer Science at Dickinson State University. Prof. Fries earned a BS in Mathematics at NDSU and then an MS and PhD, with an emphasis on representation theory and algebraic geometry, at Northeastern University. He served as Associate Professor at Eastern Nazarene College for 12 years and as Chair of Mathematics, Physics and Computer Science.

USAF Maj. Gen. (Ret.) Robert H. Latiff, PhD, is an adjunct professor at the University of Notre Dame and George Mason University with a PhD in Materials Science from the University of Notre Dame. Maj. Gen. Latiff served in the military for 32 years. Assignments included Commander of the NORAD Cheyenne Mountain Operations Center and also Director, Advanced Systems and Technology and Deputy Director for Systems Engineering, National Reconnaissance Office. Since retiring in 2006, Maj. Gen. Latiff has consulted for the U.S. intelligence community, corporations and universities in technological areas, such as data mining and advanced analytics. He is the recipient of the National Intelligence Distinguished Service Medal and the Air Force Distinguished Service Medal. Maj. Gen. Latiff's first book, *Future War: Preparing for the New Global Battlefield*, was published by Alfred A. Knopf in 2017. His second book, *Future Peace*, was published by the University of Notre Dame Press on March 1, 2022.

Alain Loukaka, PhD, earned a BS in IT Networking, with an emphasis on cybersecurity, at Clayton State University, an MS in Information Technology at Florida Tech University and then a PhD in the Information Security and Information Assurance at Capella University. His exploratory research focused on cybersecurity exploits and advanced detection methods beyond current know applications. Loukaka has worked in the IT field for more than 15 years and plans to promote better security approaches and deterrents. For the last two years, he has served as an Application Support Consultant at the Oracle Corporation.

Asad Waqar Malik, PhD, currently works as a postdoctoral scholar at NDSU's Department of Computer Science. He also serves as an Associate Professor at the School of Electrical Engineering and Computer Science at the National University of Sciences and Technology (NUST) in Pakistan. He earned a PhD in parallel and distributed simulation/systems at NUST. Prof. Malik's primary areas of interest include distributed simulation, cloud/fog computing, autonomous vehicles and the Internet of Things, with a focus on security.

Thomas Marple served as an Associate Professor of Graphic Design and Communications at Bismarck State College, where he taught for 14 years. Prof. Marple earned a Bachelor of Applied Science (BASc) from NDSU. Prior to BSC, he worked as a Conservation Engineering Technician for the U.S. Department of Agriculture. Prof. Marple also volunteers for the 1,000-mile Iditarod Trail Sled Dog Race in Alaska.

Patrick J. McCloskey is the Director of the Social and Ethical Implications of Cyber Sciences at the North Dakota University System and serves as the editor of Dakota Digital Review. Previously, he served as the Director of Research and Publications at the University of Mary and editor of 360 Review Magazine. He earned a BA in Philosophy and Political Philosophy at Carleton University and an MS in Journalism at Columbia University's Graduate School of Journalism. McCloskey has written for many publications, including the New York Times, Wall Street Journal, National Post and City Journal. His books include *Open Secrets of Success: The Gary Tharaldson Story; Frank's Extra Mile: A Gentleman's Story;* and *The Street Stops Here: A Year at a Catholic High School in Harlem,* published by the University of California Press.

Mark P. Mills is a Manhattan Institute Senior Fellow, a Faculty Fellow in the McCormick School of Engineering at Northwestern University and a cofounding partner at Cottonwood Venture Partners, focused on digital energy technologies. Mills is a regular contributor to Forbes.com and writes for numerous publications, including City Journal, The Wall Street Journal, USA Today and Real Clear. Early in Mills's career, he was an experimental physicist and development engineer in the fields of microprocessors, fiber optics and missile guidance. Mills served in the White House Science Office under President Ronald Reagan and later co-authored a tech investment newsletter. He is the author of *Digital Cathedrals* and *Work in the Age Robots.* In 2016, Mills was awarded the American Energy Society's Energy Writer of the Year. On November 2, 2021, Encounter Books published Mills's latest book, *The Cloud Revolution: How the Convergence of New Technologies Will Unleash the Next Economic Boom and A Roaring 2020s.*

Shawon S. M. Rahman, PhD, is a Professor of Computer Science and Engineering at the University of Hawaii at Hilo. He earned a BS in Chemical Engineering at Bangladesh University of Engineering & Technology, and an MS in Computer Science at NDSU and a PhD in Software Engineering also at NDSU. Prof. Rahman serves as the editor-in-chief of the International Journal on Cryptography and Information Security. He has also published more than 125 peer-reviewed articles. Prof. Rahman's research interests include information assurance and security, digital forensics, software engineering education, software testing & QA, cloud computing, mobile application development and web accessibility. He belongs to many professional organizations, including IEEE, ACM, ASEE, ASQ, ISACA, ISCA and UPE.

Jeremy Straub, PhD, is an Assistant Professor in the Department of Computer Science at NDSU and a Faculty Fellow at NDSU's Challey Institute. His research spans a continuum from autonomous technology development to technology commercialization to asking questions of technology use ethics, and national and international policy. Prof. Straub has published more than 60 articles in academic journals and more than 100 peer-reviewed conference papers. He serves on multiple editorial boards and conference committees. Prof. Straub is also the lead inventor on two U.S. patents and a member of multiple technical societies.

DAKOTA DIGITAL REVIEW SPONSOR

Marlo Anderson, cofounder of Q1Network and founder of National Day Calendar, hosting his weekly show, "Tech Ranch," on Super Talk 1270.