Received January 28, 2020, accepted January 31, 2020, date of publication February 5, 2020, date of current version February 14, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.2971960*

# Perspective: The Cyber Frontier and Infrastructure

**MIKHAIL V. CHESTER AND BRADEN R. ALLENBY**
Metis Center for Infrastructure and Sustainable Engineering, School of Sustainable Engineering and the Built Environment, Arizona State University, Tempe, AZ 85287-3005, USA

Corresponding author: Mikhail V. Chester (mchester@asu.edu)

This work was supported in part by the National Science Foundation's Urban Resilience to Extremes Sustainability Research Network under Grant 1444755, and in part by the Office of Naval Research under Grant N00014-18-1-2393.

**ABSTRACT** The accelerating integration of cyber technologies into physical infrastructure systems has radical implications for the operation, management, and vulnerabilities of our critical systems. Viewing the embedding of smart technologies in infrastructure as simply an interconnectedness of systems is insufficient. The acceleration of the coupling may represent a profound shift in the relationships between humans and their services. It lays the groundwork for explosions of artificial intelligence, new capacities for services, radical changes in efficiency, and new vulnerabilities. Yet we continue to approach infrastructure design and management with principles that don't reflect this new paradigm. To frame the challenges associated with modernizing infrastructure for accelerating cyberphysical relationships, we describe the new capabilities and vulnerabilities, and changes in approaches and thinking that are needed for the emerging complexity. We conclude by describing how infrastructure education and training will need to fundamentally shift from a focus on managing complicated physicals systems to working within complex cyberphysical systems that are likely to be governed by software.

**INDEX TERMS** Cyber security, cyberphysical systems, infrastructure, technology.

## I. INTRODUCTION

The benefits of cybertechnologies integrated into infrastructure are becoming clearer. In 2017 the City of San Diego saw energy use drop by 60% after LEDs were installed downtown in conjunction with optical, auditory, and environmental sensors. In 2018 the Arizona Department of Transportation reported that more than a dozen wrong way drivers were prevented from entering freeways by new thermal cameras and warning systems. California in late 2019 released an early warning system, providing residents with precious additional seconds to find safety before an earthquake. The increasing integration of cybertechnologies into infrastructure is creating vulnerabilities that we haven't ever experienced. A few days before Christmas in 2015 operators in the Prykkarpatyaoblenergo electric utility watched as their Supervisory Control and Data Acquisition (SCADA) system mouse pointer moved across the screen, no longer under their control, disabling substation after substation shutting down power across Ukraine. In 2017 hackers were able to access and transfer a casino's data using a vulnerability exploit in a wifi connected fish tank sensor used to regulate water temperature, food, and water quality. In 2019 a randsomware attack brought the City of Baltimore's data management systems to a halt, suspending critical services related to real estate and communications. Our increasingly connected systems are a new frontier for infrastructure, one that offers remarkable new capabilities to deliver new or augmented services and lower costs, while on the other end, creating radically new vulnerabilities that have never been faced or even conceived. The integration of cyber and physical systems is accelerating. Yet the tools that we have at our disposal to manage this integration and the outlook that we have about what this integration means remain rooted in the past century.

The number of devices that are now connected is exploding, and infrastructure is part of the trend. Estimates vary but generally show acceleration of growth in both the number of connected devices and the amount of data being transferred. Devices and data are growing faster than the global population and number of internet users [1]. There are currently around 22 billion connected devices (approximately 3 per planetary citizen) with expectations of roughly 30 billion by 2022. The growth in information traffic is outpacing that of devices. Mobile traffic has grown 17 fold

The associate editor coordinating the review of this manuscript and approving it for publication was Jenny Mahoney.

between 2012 and 2017, and mobile devices are projected to average 10.7 gigabytes of data traffic per month by 2022, up from 2.3 gigabytes in 2017 [2]. The amount and quality of data (e.g., video resolution) being transmitted is increasing [1], [3]. Specific to infrastructure, the growth in machine-to-machine technologies (M2M) are of particular interest, with a projected 34% annual growth rate to 2022 [1]. M2M refers to the direct communication between devices, which has been transitioning from closed network models to open allowing devices to avoid communications hub and instead communicate directly with a centralized system or users (creating the potential for new technologies such as autonomous connected vehicle fleets). This category of interconnected devices has the largest growth, more than smart phones and personal computers. These devices are projected to drive much of the interconnectedness of smart cities and their infrastructure.

Viewing the embedding of smart technologies in infrastructure as simply an interconnectedness of systems is insufficient, if not irresponsible. The accelerating of the coupling may represent a singularity, a profound shift in the relationships between humans and their services [4]. It lays the groundwork for explosions of artificial intelligence, new capacities for services, radical changes in efficiency, and with those new vulnerabilities. At the infancy of this shift, our comprehension of the implications of an accelerating cyberphysical world remains limited, and as such our ability to manage the implications and protect against vulnerabilities is likely woefully lacking. This unpreparedness has major implications for infrastructure managers and engineering education. It raises questions as to whether the next generation of leaders have the appropriate competencies to steer infrastructure as it transitions.

It's important to understand the context in which the acceleration of the interconnectedness between cyber and physical systems is happening. The demand for services delivered by infrastructure is one side of the story. Physical infrastructure systems (water, power, transportation, etc.) have largely been built to provide services that have for decades been relatively stable. We want water from a faucet the same way we did a century ago. How we demand electricity hasn't changed much from 1882 when Edison begin providing power through his Pearl Street Station to lower Manhattan. And over the past 70 or so years we (particularly those in the U.S.) have largely demanded automobility, and the associated transportation infrastructure that hasn't radically changed in technology (but certainly extent) in this time. As such, the technologies that make up the backbone of our physical infrastructure systems have remained relatively stable for decades, if not centuries [5]. Certainly new technologies have been added, and efficiencies introduced, but water mains, pumps, transmission lines, transformers, and asphalt continue to dominate the core structure and functioning of these systems. If we were to bring Thomas Edison to today in a time machine he'd largely understand the power grid. But if we were to show Alexander Graham Bell a modern smart phone he'd be flummoxed by the black mirror. The acceleration of cyber technologies means that the cycle time (how quickly a past generation is replaced by a new generation) is now outpacing that of infrastructure. This is part of the challenge, working with cyberphysical systems that can't be treated as traditional coupled systems, given that cyber is cycling faster and faster than the physical.

Concurrent with the technological change and increasing coupling of cyber and physical systems, there has been rapid acceleration in other fields, as well as social and political structures. Massive advances in computational power, data storage, and data analytics are driving advances in artificial intelligence and social media. At the same time we've seen a shift in military policy with a rise in asymmetric warfare strategies by nation states with weaker hardware, smaller armies, or less prepared armies that engage in cyberattacks to affect the strategic balance of power [6], [7]. Nation-states have adopted explicit strategies of civilizational conflict which make all of society's systems, from finance to infrastructure to health, targets [8]. The combination of rapid advancement of digital technologies, increasing interconnectedness of cyber and physical systems, different outlooks on humans, and differing approaches to warfare, represents a radically new paradigm, and infrastructure is at the center. We can't ignore this context as we design and manage infrastructure going forward.

Towards providing insights into the design and management of infrastructure in a future with potentially new demands for services, vulnerabilities, and relationships between people, the environment, and technologies, we explore the changing cyberphysical dynamics and its implications. We start by exploring technological acceleration theory and what that means for infrastructure. Next, we describe how transitions from physical to cyberphysical infrastructure will create new capabilities, and vulnerabilities. We consider the changing relationship between people and their services as mediated by infrastructure, as we accelerate the cyber integration of physical systems. We conclude by recommending how infrastructure education and management must shift from models that emphasize systems as they've been to systems that will be controlled by cyber technologies.

We discuss three coupled but conceptually different systems: 1) cyber and Information and Communication Technology (ICT) infrastructure; 2) physical infrastructure, that increasingly includes ICT functionality and technology; and 3) the ''institutional context'' of infrastructure (including education and management). We don't view this article as an exhaustive exploration or summary of all of the issues relevant to cyberphysical systems, but more so an effort to elucidate new thinking about the rapidly changing relationship between technologies, infrastructure and people.

## II. ACCELERATING INTELLIGENCE

In 1999 Ray Kurzweil noted that many technologies tend to grow exponentially and as such the 21st century can be expected to yield 20,000 historical years of relative progress [4]. He branded this phenomenon as the Law of Accelerating Returns, which if true is accelerating humankind towards technological change so radical and profound that we cannot comprehend the implications. The Law of Accelerating Returns is a theory of change acceleration, which in general describes the increasing rate of technological progress that ultimately results in profound social and cultural change; many theories of change acceleration exist [4], [9]–[11]. While technology has always moved forward, the rate at which technology has changed up until recent times has mirrored population growth, meaning that essentially all of the world's population remained at subsistence levels of production and consumption [12], [13]. But at the dawn of the 21st century evidence accumulates that technological change is now increasingly exponentially, representing a new paradigm for humans and the systems they operate [14], [15]. This acceleration creates remarkable new opportunities, and also hazards and vulnerabilities, and implies a future that is difficult to meaningfully comprehend. How long such an acceleration can proceed has been the subject of much debate [16]. However, as we look forward at the coming century there is accumulating evidence to warrant a critical examination of the implications of technological acceleration [15]. Technological acceleration is attributed to positive feedback loops, and trends of increasing integration of cyber into physical systems raise questions of whether the perceived benefits of cyber result in integration in infrastructure that thereby changes services and vulnerabilities creating new cyber-integration demands.

### A. MATURATION OF CYBER TECHNOLOGIES

Infrastructures have, for decades, operated as either purely physical systems or with limited and often isolated computing capabilities, frequently included in system design as mechanical devices (inertial and centrifugal governors on steam engines might be regarded as a form of computational device, for example). More recently, sensors, software, and digital controls (including SCADA) have been increasingly used since the latter half of the twentieth century, but these digital systems largely functioned to augment the core underlying infrastructure which, for decades, if not longer have been largely driven by physical systems and hardware. But recent advances in hardware and software are driving the accessibility, usability, and cost of cyber-technologies down. Rajkumar [17] provides a useful synthesis of the factors that are pushing and pulling cyber technologies leading to their ubiquity. Sensors are now available to measure the properties at nano to macro scales. Actuators have become ubiquitous (again across scales). Alternative energy sources are maturing. Satellite and wireless communications are available across the globe, and internet connectivity is growing. At the same time, computing and storage capabilities are improving, and appearing in ever smaller form factors. Demand for these technologies is also growing. Building and environmental controls, critical infrastructure monitoring, process control, factory automation, healthcare, aerospace, and defense are all advancing cyberphysical systems as industries strive for radical new capabilities and efficiencies. The result is a new paradigm of infrastructure that includes hardware, software, firmware, and wetware (people) integrated into new techno-human infrastructure. These systems are now smart and connected, delivering the ability to measure system, natural, and human dynamics, in ways that weren't feasible a short time ago. They are able to generate, see, and make sense of massive data streams (often using integrated AI/human capabilities), and send data to users in real time, in ways that heretofore have not been possible. This changing paradigm will shift how we interact with infrastructure and what we ask them to do.

The proliferation of lower cost, smaller, more efficient, and more powerful computing technologies coupled with data transfer, storage, and management technologies, and supported by emerging techniques to make sense of voluminous and federated datasets, including AI, represents profound new capabilities and efficiencies for physical systems [17]. This confluence of technologies represents an important transition period for infrastructure. Prior to this maturation we typically think of infrastructure as largely ''dumb'' physical systems absent of powerful and connected systems driven at large scale by software intelligence [18]. The proliferation of the internet and augmentation of communication capacities (including bandwidth and communication protocols) has resulted in radical new possibilities for physical systems. These new technologies represent new capabilities for how we understand and interact with natural and human systems.

### B. BENEFITS OF CYBERPHYSICAL SYSTEMS

Indeed the integration of cyber and physical systems creates new capabilities that didn't exist before. But it is what these capabilities enable that drive the accelerating integration of the systems. Prior to discussing infrastructure at broad scales it is useful to examine a parallel but smaller technology and its integration of cyber and physical systems, the automobile. Until the 1950s automobile technologies had no cyber technologies; they were purely mechanical systems linked to each other via other mechanical systems or controlled through the cognitive capacities of the driver. The first sensors integrated into cars simply alerted drivers to problematic conditions such as low oil pressure or charge via a dashboard light [19]. But critical system functioning was controlled by valves and other mechanical devices that responded directly to the driver's input. In 1968 Volkswagen introduced the first microchip into a car to control fuel injection and minimize emissions, a device now known as an Electronic Fuel Injector (EFI). Today's EFIs take in readings from dozens of subsystem sensors, perform millions of calculations per second, and adjust the spark timing and how long the fuel injector is open, ensuring the lowest emissions and highest fuel economy [20]. By 1999 cars had dozens of microprocessors [21]. Today, sensors, processors, cameras, accelerometers, and other technologies result in 65Mb/s of data transferred throughout a vehicle, roughly 2 miles of cabling, and 280 connections to manage power and that data [22]. It's naïve to think that pushing a gas pedal directly engages the engine. Instead a computer determines based on your past behavior, environmental conditions, and readings from the vehicle how to give you the best ride. But this is just one scale of the system. Navigation software (e.g., Google Maps) now takes into account thousands of other drivers and routes you based not simply on the shortest travel time in an unloaded network but with consideration of how all other users of the system are traveling. Hybrid electric vehicles can learn your frequent destinations and automatically switch to electric power as you approach those destinations, thereby saving you on gas [23]. The integration of cyberphysical systems across scales as they relate to the automobile, the efficiencies they introduce, and the new capabilities radically alter our relationship with mobility services.

Cyberphysical infrastructure allow for new capabilities to optimize systems across broad scales and time frames, create new efficiencies, and create multifunctionality where it didn't exist before. Consider the telephone, initially a handset on a dedicated circuit that offered only voice communication, whereas a modern mobile phone provides voice, text, video, music, picture taking capability, games, and a myriad of other apps all on one physical device, driven over one communications infrastructure. Fundamentally, the integration of cyber into physical systems creates new cognitive capacity about the system by shifting it towards relying more critically on information. New insights are created about not only the internal functioning and relationships between subsystems but also the demands (needs) being placed for the services. New optimization techniques are created with the integration of cyber creating the potential for efficiency gains. Sensors that detect ambient light can be used to control whether traffic lights are on or off, and their intensity when they're on, thereby reducing the need for electricity. Realtime information driving forecasts for electricity demand (power is perhaps the most historical major cyberphysical infrastructure) allows operators to deploy supply as needed. And in the case of mobility, a large scale connected vehicle fleet (possibly through Google Maps and emerging vehicle-to-vehicle communication technologies) offers the potential to shave peak demand thereby reducing the need for new infrastructure and changing the kind of infrastructure that transportation engineers need to think about. Parking lots become less important; charging stations become more important. These are possibilities that we can comprehend. With the deployment of artificial intelligence into cyberphysical systems the capabilities with full autonomy and humans not in control are beyond comprehension. But even today and in the near future, before the advent of AI, we must recognize that each new capability brings with it the potential for vulnerabilities and exploits.

## III. VULNERABILITIES

With great promise comes the potential for radically new vulnerabilities, the likes with which we have never seen with infrastructure. These vulnerabilities arise not simply because new exploits are created, but are largely due to the new capabilities for exploiting operators, users, control systems, distributed software, and hardware. These vulnerabilities arise at a time when cyberattack tools have become available to low-expertise hackers and nation-states have established and tested strategies, and established resources for asymmetric warfare.

### A. TAXONOMIES OF THREATS

To understand how cyber threats emerge in infrastructure a taxonomy is helpful. Many taxonomies exist for cyber threats, differing depending on the phase of the hacking process (data collection, storage, processing, etc.), target, actors, methods, techniques, or capabilities [24]. There is no preeminent taxonomy for threats to cyber-infrastructure systems. To understand these threats it is helpful to first take a perspective within an infrastructure risk model. NIST's Guide for Conducting Risk Assessments provides a helpful model for framing risk factors for infrastructure management. Cyber threat taxonomies can map to the risk processes in NIST's model providing a roadmap for analyzing threats as they relate to infrastructure. Starting with the threat source, taxonomies describe the types of actors involved in attacks including professional criminals, state actors, terrorists, cyber vandals, hacktivists, internal actors, and cyber researchers [25]. They may focus on the threat event and techniques used including degree of automation, exploited weakness, source address validity, possibility of characterization, attack rate dynamics, impact on the victim, victim type, and persistence of agent [26]. The attack vector, vulnerability, and exploit have also been the focus of taxonomies. Hansman and Hunt [27] catalog and map the types of attacks to targets (including hardware and software exploits) and the corresponding vulnerabilities. Harry and Gallagher [24] focus their taxonomy on the impacts of attacks by describing the outcomes of disruptions of operations and illicit acquiring of information. Figure 1 shows how organizational risk is a result of different sources of attacks, event types, impacts, and vulnerabilities.

While the level of sophistication and number of attacks has increased over time, the intruder expertise has decreased. This trend reflects the growing availability of tools to cyberattackers. While in the past considerable expertise and resources were needed to conduct an attack, it is becoming more and more common for a small number of expert hackers to make their tools available to a broader community of novice hackers. This growing body of cybercriminals has the capability of deploying an arsenal at ever increasing scales, diversity, and sophistication with increasingly devastating effects [27], [31], [32]. This trend reflects a new reality of cyberattacks. As U.S. National Intelligence Director James Clapper testified "Rather than a 'Cyber Armageddon' scenario that debilitates the entire US infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyber attacks from a variety

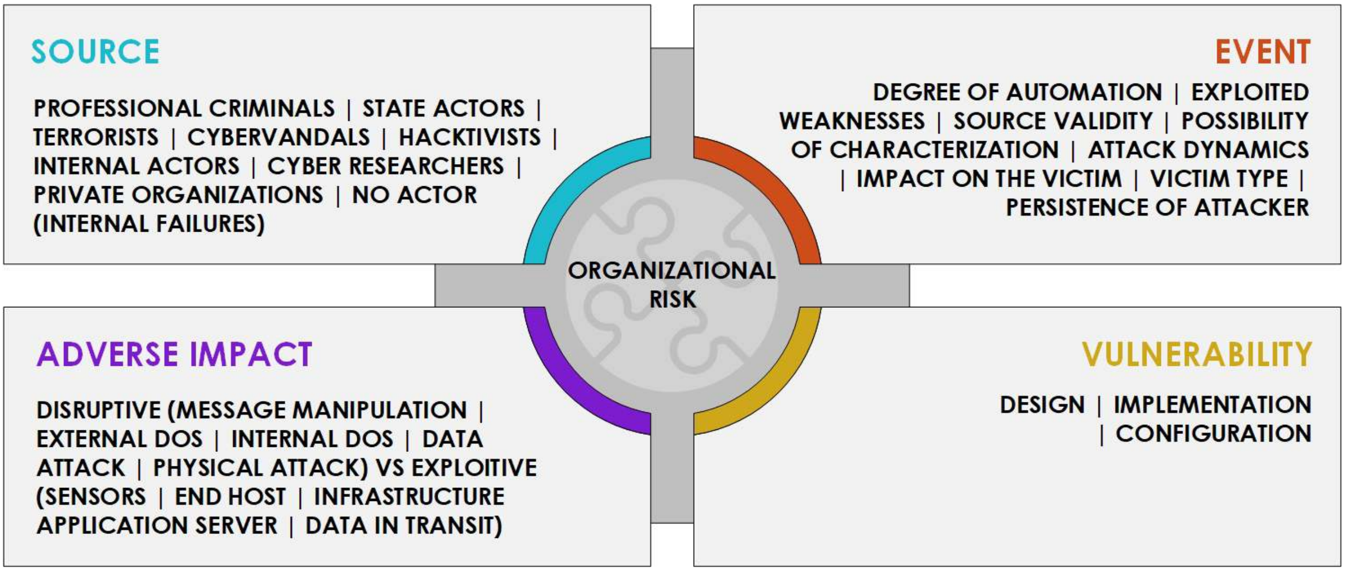
SOURCE
PROFESSIONAL CRIMINALS | STATE ACTORS | TERRORISTS | CYBERVANDALS | HACKTIVISTS | INTERNAL ACTORS | CYBER RESEARCHERS | PRIVATE ORGANIZATIONS | NO ACTOR (INTERNAL FAILURES)
EVENT
DEGREE OF AUTOMATION | EXPLOITED WEAKNESSES | SOURCE VALIDITY | POSSIBILITY OF CHARACTERIZATION | ATTACK DYNAMICS | IMPACT ON THE VICTIM | VICTIM TYPE | PERSISTENCE OF ATTACKER
ORGANIZATIONAL RISK
ADVERSE IMPACT
DISRUPTIVE (MESSAGE MANIPULATION | EXTERNAL DOS | INTERNAL DOS | DATA ATTACK | PHYSICAL ATTACK) VS EXPLOITIVE (SENSORS | END HOST | INFRASTRUCTURE APPLICATION SERVER | DATA IN TRANSIT)
VULNERABILITY
DESIGN | IMPLEMENTATION | CONFIGURATION

**FIGURE 1.** Risk Model, Key Risk Factors and Associated Exemplary Taxonomies. Based on: [24]–[30].

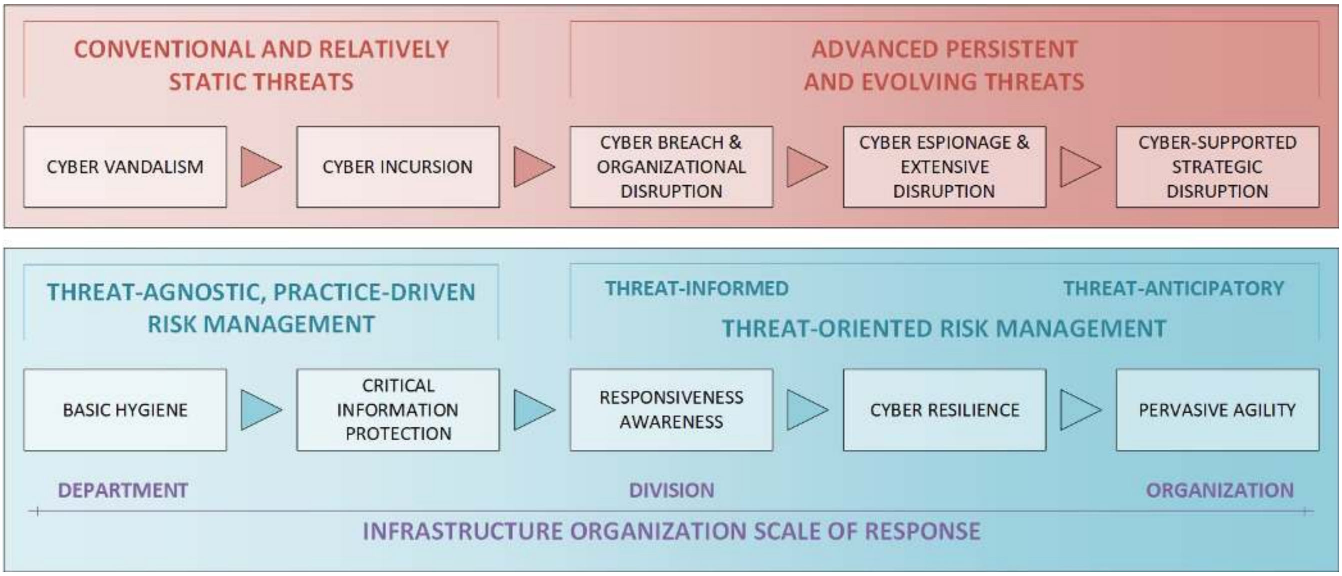
CONVENTIONAL AND RELATIVELY STATIC THREATS
ADVANCED PERSISTENT AND EVOLVING THREATS
CYBER VANDALISM
CYBER INCURSION
CYBER BREACH & ORGANIZATIONAL DISRUPTION
CYBER ESPIONAGE & EXTENSIVE DISRUPTION
CYBER-SUPPORTED STRATEGIC DISRUPTION
THREAT-AGNOSTIC, PRACTICE-DRIVEN RISK MANAGEMENT
THREAT-INFORMED
THREAT-ANTICIPATORY
THREAT-ORIENTED RISK MANAGEMENT
BASIC HYGIENE
CRITICAL INFORMATION PROTECTION
RESPONSIVENESS AWARENESS
CYBER RESILIENCE
PERVASIVE AGILITY
DEPARTMENT
DIVISION
ORGANIZATION
INFRASTRUCTURE ORGANIZATION SCALE OF RESPONSE

**FIGURE 2.** Sophistication of cyber threats (red), risk management strategies (blue), and where in a typical infrastructure divisional bureaucracy responsibility for managing the risk may lie (purple). Adapted from [29].

of sources over time, which will impose cumulative costs on US economic competitiveness and national security'' [33]. The ongoing low to moderate level attacks may reflect a Death by 1000 Cuts civilizational conflict strategy [8], or simply that the vulnerabilities inherent in today's cyberdesigns attract an ever-increasing number of unrelated attacks.

The level of sophistication of the attacker directly informs the strategies that should be developed when preparing for a cyberattack (Figure 2). Conventional threats include cyber vandalism and incursion often involving disgruntled or suborned insiders, denial-of-service attacks, and hackers who have obtained legitimate user credentials [29]. Conventional threats can be approached by practice-driven risk management strategies that largely focus on basic hygiene and critical information protection (protocols for password changes, software updates, hardware updates, software installations, limiting users, and backing up data). Advanced threats represent cyber adversaries that learn and evolve, such that compliance and good-practice driven strategies are insufficient, and new competencies and threat-specific knowledge are needed (actors capable of such sophisticated cybercampaigns, such as Russia's Cozy Bear, are known as Advanced Persistent Threats) [29]. While conventional threats can often be handled by a properly trained IT department, advanced threats may require sustained and directed resources for cybersecurity and management of corresponding initiatives, and appropriate staff, tools, and strategic planning. Agility may be required to consider the goals of attackers, the techniques the attacker may use, and the appropriate anticipatory and reactive responses an organization can deploy to protect itself.

### B. COMPLEXITY AND VULNERABILITY

As our infrastructure systems evolve towards greater complexity, in many ways defined by the increasing coupling of cyber and physical systems, vulnerabilities will need to be managed differently. We define infrastructure complexity here as the changing technical, environmental, and social context that engineers and managers must navigate to deliver and evolve services [34]. What is particularly interesting about the complexity associated with infrastructure is the speed and scale of which other systems are being integrated. The changing relationship of infrastructure users with the systems they rely on (e.g., the availability and price of parking spaces, the real-time arrival of the next transit vehicle, how to reroute to avoid traffic, the timed use of low-cost electricity by home appliances, the number of infrastructure elements that are offline in their region) through apps and internet connected services is exploding, fundamentally altering people's understanding and thereby use of services [35].

With the new possibilities created through cyberphysical systems comes vulnerabilities and exploits that didn't exist before, some of which transcend the cyberphysical system. It's possible to conceive of cyber attackers no longer needing to target the cyberphysical system itself, but instead conditioning operators with targeted disinformation. Most attacks on infrastructure occur from within, generally disgruntled employees with internal access [36]. In 2006 engineers sabotaged intersection controls in Los Angeles, and in 2000 an ex-employee disabled critical SCADA systems with the hopes of being re-hired to fix the problem [37], [38]. With new means for engaging with these operators, e.g., through social media, we can conceive of a new method for inciting sabotage without directly engaging with the infrastructure. In 2019 utility operators were targeted with emails impersonating their accreditation society baiting them to open malware attachments masked as notifications that their professional credentials were being revoked [39]. The attachments contained the LookBack virus that would give the cyberattackers access to the utility's systems. Another vulnerability that is receiving considerable attention is the controlling of outgoing information about an attack to distort facts and condition a particular response. Reflexive control (the means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action), a principle developed by Russia since the 1960s, is particularly well-suited for the hyper-connected and information rich era [40]. The case of the 2015 Ukranian power grid cyberattack, for example, was part of a broader Russia strategy that involved denial of service attacks, disinformation campaigns (including social media, mass media, and internet trolls), and energy diplomacy (involving coercion that forced Ukraine to pay market prices for oil and gas), that together sowed disinformation across international outlets. The strategy allowed Russia to deploy minimal forces thereby staying below the threshold for international intervention, while achieving their objective of stopping a revolution that threatened to overturn the pro-Russian administration [41], [42].

The possibilities for impact are no longer limited to the systems themselves, but span the interconnected systems in which our technical systems function. A challenge remains that those who understand the threat landscape and the complex tools being deployed are largely disconnected from those making day-to-day decisions about infrastructure. While in the U.S. the National Institute of Standards and Technology and Department of Homeland Security issue valuable guidelines and recommendations for how to prepare for and protect against cyberattacks [28], [43]; the reality of infrastructure at the ground level is one of limited resources and governing institutions that are structured to operate towards reliability principles that in many ways are designed to deliver services as they've been delivered in the past (and the existing engineering education structure reflects this).

### C. CYBERWARFARE NORM

That cybersecurity has become a major challenge for engineered systems is neither new nor particularly surprising. The roots of the challenge lie deep in recent geopolitical history. Partially because the United States was the strongest country left standing after World War II and the collapse of the Soviet Union, and partially because defense expenditures by the United States have consistently been far greater than those of any rival, the conventional military forces of the United States are generally understood to be stronger than those of any other power [44]–[47]. This dominance has driven adversaries, especially state adversaries such as Russia and China, to adopt asymmetric warfare strategies that redefine conflict away from traditional military engagement to longer term ‘‘civilizational conflict’’ which among other things, elevates information warfare, disinformation and subversion techniques, and weaponized narrative to priority attack mechanisms [8], [48], [49]. In perhaps the most cited military strategy article of the past decade, General Valery Gerasimov, Chief of the General Staff of the Russian Federation, notes that in the twenty-first century there has been ‘‘a tendency toward blurring the lines between the states of war and peace,’’ and that ‘‘a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war.’’ Writing before the successful Russian invasion of Crimea and Eastern Ukraine, General Gerasimov emphasizes [50]:

‘‘The very ‘‘rules of war’’ have changed. The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.... The focus of applied methods of conflict has altered in the direction of the broad use of political, economic, informational, humanitarian, and other nonmilitary measures—applied in coordination with the protest potential of the population. All this is supplemented by military means of a concealed character, including carrying out actions of information conflict and the actions of special operations forces. The open use of forces—often under the guise of peacekeeping and crisis regulation—is resorted to only at a certain stage, primarily for the achievement of final success in the conflict.''

Russia is not alone in developing civilizational conflict strategies as an asymmetric response to American conventional dominance. Shocked by the success of allied forces in Desert Storm (1990-1991), Chinese strategists have developed a strategy of ''Unrestricted Warfare'' that contemplates conflict across the entire domain of a civilization, from financial markets to all forms of infrastructure [47]:

''[T]here is reason for us to maintain that the financial attack by George Soros on East Asia, the terrorist attack on the U.S. embassy by Usama Bin Laden, the gas attack on the Tokyo subway by the disciples of the Aum Shinri Kyo, and the havoc wreaked by the likes of Morris Jr on the Internet, in which the degree of destruction is by no means second to that of a war, represent semi-warfare, quasi-warfare, and sub-warfare, that is, the embryonic form of another kind of warfare.''

Iran, North Korea, and others are following in Russian and Chinese footsteps, although not as part of such a structured and formal geopolitical conflict strategy.

The complacency of academic engineering education institutions in light of active cyberwarfare directed at essentially all engineered systems within American, and Western, society is remarkable, and untenable. Engineering students in disciplines from civil and environmental, to biomedical, to industrial engineering are taught to include ever more advanced sensor, computing, communication, and data processing systems in their designs because of concomitant dramatic improvements in function and efficacy. But they are taught next to nothing about information and cybersecurity, both because of the remarkable inertia of engineering curricula to any proposed change, and because their professors were never trained in the subject, are not versed in it, and completely fail to perceive, much less understand, relevant geopolitical shifts. The result is that American engineering education is optimally designed to create a generation of engineering professionals who will, among other things, unknowingly design ever more vulnerability and frailty into the built environment and infrastructure systems that are critical to our society. We should recognize that the integration of cyber technologies into infrastructure is altering the relationships between people and their services.

## IV. HUMANS, THEIR SERVICES, AND THE ENVIRONMENT, MEDIATED BY SOFTWARE

Edwin Hutchin's 1995 book *Cognition in the Wild* describes, through the lens of U.S. Navy pilots and sailors, the differences in cognitive approaches between individuals with no technology (the first sailors) and groups with technology [51]. Hutchins argues that cognition in modern society is composed of multiple agents and their technologies. While sailors on a modern Navy vessel cannot necessarily navigate like early sailors with no technology, they are able to accomplish remarkably more, by compartmentalizing tasks, communicating effectively, and utilizing technology. Technology creates new opportunities for understanding the world around us, and as it accelerates is likely to create radical new relationships between people and their environments.

The rapid integration of cyber technologies into infrastructure and the implications for how humans interact with and demand services may represent a fundamentally new relationship that remains difficult if not impossible to comprehend. Whereas in the past new technologies often represented new capabilities and efficiencies, the hyperconnected and information-driven reality represents a radical change in how we see and experience the world. And artificial intelligence that mediates our interactions with other people, information, and services is positioned to fundamentally alter human experience. Infrastructure are at the center of this change.

Physical infrastructure systems will remain the backbone for cybertechnologies, but how they're used is poised to radically change. Several key dynamics may reshape our relationships with infrastructure:

- **Physical Systems as the Cyber Backbone**: Despite shifts from hardware to software functionality that reduces the need for physical assets [52], core physical systems will be needed to enable information transfer, analytics, and storage. And who controls the core physical systems will be economically and politically strategically positioned (see Google and Facebook's efforts to deploy fiberoptic lines around the world and recent concern over 5G cellular hardware security) [53], [54].
- **Insights into Infrastructure Services**: Next, people are and will continue to gain new insights about infrastructure that they didn't have before, thereby changing how they demand infrastructure services. The advent of smart phones created an industry of location tracking and traffic analysis firms that are now delivering products and new insights to travelers about the conditions of roads, how to route to minimize delays, and how to change their travel behaviors to reduce trip times [55]–[57]. While still in its infancy, the possibilities of software making sense of the complexity of the transportation system has remarkable implications for how we use the system based on how the software understands it. Imagine similar insights and software-driven intelligence behind water and energy use, for example. And we are already heavily debating and seeing the implications of such intelligence driving how we consume news and media [58].
- **Evolving Demands for Infrastructure Services**: While it's easy to imagine how new and improved information can make our interactions with infrastructure more efficient (e.g., saving us travel time by rerouting to a path we would

have never considered, or managing our appliances to run at low-cost electricity times of day), it's likely that the possibilities offered by cyber technologies will result in demands for new services. The emergence of car, bicycle, and scooter sharing, which is resulting in major changes to how people travel in many major cities [59], would not have been possible without smart phones and cellular networks. Furthermore, combining modalities with autonomous vehicles means that you end up needing to redefine the urban transportation network completely.

- **Adaptive Capacity**: The integration of sensing technologies coupled with analytical capabilities and software-based intelligence is likely to create new adaptive capacities for infrastructure. Sensors of various forms that can detect the conditions of assets in the system, both in terms of structure and function, are already being deployed and utilized in new ways. This information will likely drive algorithms that make sense of the overall state of the system, and decisions about how to manage assets to ensure integrity and efficiency. Imagine a SCADA system deciding to triage a portion of a water distribution network where a pipe is expected to fail to ensure that a cascading failure does not ensue. This capability will likely increase the agility and flexibility of infrastructure services to meet more rapid changes in conditions, and respond to hazards. Google Maps may already be showing us this adaptivity, by routing users with considerations of larger systems dynamics when there is a traffic accident.

These changes represent just a few of the possibilities of how cyber technologies may change our relationship with infrastructure. Preparing infrastructure managers and engineers for these shifts is critical to ensuring the integrity and safety of cyberphysical systems. As the technologies that define infrastructure change, so must education and governance for these systems.

## V. PREPARING FOR CYBERINFRASTRUCTURE

Several critical and immediate efforts are needed to ensure that the integration of cyber-infrastructure results in systems that continue to support society's needs and are safe and secure. While there are certainly hardware and software changes that are needed, we focus these efforts on the institutional management of infrastructure and the training of future managers.

The training around integrated cyberphysical systems at universities is essentially non-existent and should immediately be developed as a core competency, a Fifth Column that can change the status quo of how we view and manage infrastructure [60]. Engineers, architects, planners and other infrastructure managers will still need knowledge around fundamentals of design principles, underlying science, and operations. However, they will need to be trained with new competencies that support a new norm for infrastructure, i.e., one where systems are increasingly focused on information management [61]. Currently, disciplines such as Civil, Environmental, and Mechanical Engineering, Planning, and Architecture (domains largely responsible for the physical systems) train largely independently of Computer Science, Computer Engineering, Information Sciences, and military/security domains. This fragmentation of knowledge is likely to lead to unintended consequences, both in the relevancy of disciplines, and who and what decides how infrastructure services are managed. Cyber technology, information management, and security must become central to the training of infrastructure managers.

To attempt to manage infrastructure today without consideration of the implications of accelerating integration of cyber into the physical systems, is an ethical and professional failure, particularly in light of the increasing cyber attacks on infrastructure. Cyber security competencies must become central to the training of infrastructure managers. New managers must have at least basic competencies to know why different actors might want to target their systems, what techniques they might use to exploit vulnerabilities, and strategies that can be deployed to protect systems (Figure 2) [29]. It has become remarkable easy (both in terms of technology and cost) to layer new and connected technologies into old and new systems, without a comprehensive understanding of the implications, risk, and vulnerabilities. Infrastructure managers must be trained with the tools to understand how to vet hardware and software on devices, encrypt and secure communications, manage access to information, and thwart inside and outside attacks.

Infrastructure managers will need to develop roadmaps that guide the planning and development of their cyber systems into physical, that will require translating federal insights to their locales. It is difficult to find cyber planning and cybersecurity plans for state, regional, and local infrastructure agencies. These plans should immediately be developed and serve as a roadmap for how infrastructure agencies plan on integrating cyber into their systems and protect their systems against threats. Much of the cybersecurity literature identified was developed by federal agencies (namely NIST and DHS) and there is good reason to assume that intelligence agencies are also central to making sense of the challenge. However, when it comes to day-to-day decisions about infrastructure assets limited guidance exists. This information is sorely needed. It should be specific to region (considering local needs and hazards), describe threats across scales (from foreign to local actors), guide managers in how to access vulnerabilities in hardware and software, and provide strategies for protecting systems.

A remarkably difficult challenge will be steering infrastructure as artificial intelligence comes online. Software developers that are developing artificial intelligence appear to be doing so largely independent from those that design and manage infrastructure. The implications of this discoordination are very unclear. Will the software manage services in ways that infrastructure managers hadn't intended? Will it drive infrastructure development in an unplanned direction? Will it monopolize resources beyond the capacity of the system? For every question that we think of there's probably two more that are beyond our comprehension, given the complexity of an AI managed system and its potential for restructuring how we understand and interact with human systems. What is clear is that the tools and techniques that we currently train and deploy are badly out of date, and that the acceleration of the integration of cyber and physical systems is not likely one that we will be able to control. Instead, we'll need to accept that our new role is one of understanding and guiding the emerging complexity.

## VI. CONCLUSION

New approaches to how we think about goals and structure of infrastructure, what those systems do, and how they are operated are immediately needed to ensure that societal needs are met into the future. The cyber technologies that are increasingly integrated with physical systems are being developed faster than the infrastructure, resulting in an increasing mismatch between the new capabilities delivered by the cyber technology and the obdurate backbone physical system's capabilities. This is likely to lead to unintended consequences in how infrastructure are used and their reliability. Furthermore, the acceleration of technologies, their pervasive use, and a dearth of knowledge and training among infrastructure managers is creating major vulnerabilities that are already being exploited. Education of infrastructure managers must include cyber technology. The growing complexity of human systems and their relationships with natural and social systems appears to be accelerating and the sooner we accept that the approaches we use to manage the core infrastructure systems that support human activities are rooted in the past century, the sooner we can reinvent infrastructure management for the coming centuries.

## REFERENCES

[1] Cisco, "Cisco visual networking index: Forecast and trends, 2017–2022," Cisco, San Jose, CA, USA, White Paper C11-74149-00, 2019.

[2] Cisco, "Cisco visual networking index: Global mobile data traffic forecast update, 2017–2022," Cisco, San Jose, CA, USA, White Paper C11-738429-01, 2019.

[3] *Ericsson Mobility Report*, Ericsson, Stockholm, Sweden, 2017.

[4] R. Kurzweil, "The law of accelerating returns," in *Alan Turing: Life and Legacy of a Great Thinker*, C. Teuscher, Ed. Berlin, Germany: Springer, 2004, pp. 381–416.

[5] M. V. Chester and B. Allenby, "Toward adaptive infrastructure: Flexibility and agility in a non-stationarity age," *Sustain. Resilient Infrastruct.*, vol. 4, no. 4, pp. 173–191, Oct. 2019.

[6] J. Fritz, "How China will use cyber warfare to leapfrog in military competitiveness," *Cult. Mandala Bull. Cent. East-West Cult. Econ. Stud.*, vol. 8, no. 1, pp. 28–80, 2008.

[7] M. Hjortdal, "China's use of cyber warfare: Espionage meets strategic deterrence," *J. Strateg. Secur.*, vol. 4, no. 2, pp. 1–24, Jun. 2011.

[8] B. R. Allenby, "The paradox of dominance: The age of civilizational conflict," *Bull. Atomic Scientists*, vol. 71, no. 2, pp. 60–74, Jan. 2015.

[9] P. T. de Chardin, *The Phenomenon of Man*. New York, NY, USA: Harper Collins, 2008.

[10] R. L. Coren, *The Evolutionary Trajectory: The Growth of Information in the History and Future of Earth*. Boca Raton, FL, USA: CRC Press, 2003.

[11] L. Nottale, J. Chaline, and P. Grou, *Les Arbres de L'évolution: Univers, Vie, Société*. Hachette Littératures, Paris, France, 2000.

[12] G. Clark, *A Farewell to Alms: A Brief Economic History of the World*. Princeton, NJ, USA: Princeton Univ. Press, 2007.

[13] N. Rosenberg and L. E. Birdzell, *How the West Grew Rich: The Economic Transformation of the Industrial World*. London, U.K.: Tauris, 1986.

[14] J. Syvitski, "Anthropocene: An epoch of our making," *Global Change*, vol. 78, pp. 12–15, Mar. 2012.

[15] B. Nagy, J. D. Farmer, J. E. Trancik, and J. P. Gonzales, "Superexponential long-term trends in information technology," *Technol. Forecasting Social Change*, vol. 78, no. 8, pp. 1356–1364, Oct. 2011.

[16] J. Rennie, "Ray Kurzweil's slippery futurism," in *IEEE Spectrum: Technology, Engineering, and Science News*. New York, NY, USA: IEEE Spectrum, Nov. 2010. Accessed: Jul. 26, 2019. [Online]. Available: https://spectrum.ieee.org/computing/software/ray-kurzweils-slippery-futurism

[17] R. Rajkumar, "A cyber–Physical future," *Proc. IEEE*, vol. 100, no. Special Centennial Issue, pp. 1309–1312, May 2012.

[18] B. Allenby, "Infrastructure in the anthropocene: Example of information and communication technology," *J. Infrastruct. Syst.*, vol. 10, no. 3, pp. 79–86, Sep. 2004.

[19] R. Jurgen, *History of Automotive Electronics*. Warrendale, PA, USA: Society of Automotive Engineers, 1998.

[20] Chips Etc. *Computer Chips Inside the Car*. Accessed: Feb. 6, 2020. [Online]. Available: https://www.chipsetc.com/computer-chips-inside-the-car.html

[21] J. Turley. (1999). Embedded Processors by the Numbers. EETimes. Accessed: Jul. 26, 2019. [Online]. Available: https://www.eetimes.com/author.asp?section_id=36&doc_id=1287712

[22] A. Katwala. (2017). *Connected Cars are 'Driving Microchip Development'*. Accessed: Jul. 26, 2019. [Online]. Available: https://www.imeche.org/news/news-article/connected-cars-are-'driving-microchip-development'

[23] M. Amick. (May 19, 2013). First Drive: Lincoln's 2013 MKZ Hybrid Makes Going Green Easy, but Lacks Luxury. Digital Trends. Accessed: Aug. 1, 2019. [Online]. Available: https://www.digitaltrends.com/cars/first-drive-lincolns-2013-mkz-hybrid-makes-going-green-easy-but-lacks-luxury/

[24] C. Harry and N. Gallagher, "Classifying cyber events: A proposed taxonomy," *J. Inf. Warfare*, vol. 17, no. 3, p. 17, 2018.

[25] M. de Bruijne, M. van Eeten, C. H. Gañán, and W. Pieters, "Towards a new cyber threat actor typology," TU Delft, Delft, The Netherlands, Tech. Rep., 2017.

[26] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, p. 39, Apr. 2004.

[27] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks," *Comput. Secur.*, vol. 24, no. 1, pp. 31–43, Feb. 2005.

[28] *Guide for Conducting Risk Assessments*, document SP 800-30 Rev. 1 , Nat. Inst. Standards Technol., Washington, DC, USA, 2012.

[29] D. Bodeau and R. Graubart, "Cyber prep 2.0: Motivating organizational cyber strategies in terms of threat preparedness," MITRE, Bedford, MA, USA, Tech. Rep. 15-0797, 2017.

[30] J. Howard and T. Longstaff, "A common language for computer security incidents," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND98-8667, 1998.

[31] H. Lipson, "Tracking and tracing cyber-attacks: Technical challenges and global policy issues," Carnegie Mellon Univ. Softw. Eng. Inst., Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-2002-SR-009, 2002.

[32] *The Resilience of the Electric Power Delivery System in Response to Terrorism and Natural Disasters: Summary of a Workshop*, NRC, Washington, DC, USA, 2013.

[33] J. Clapper, "Statement for the record: Worldwide cyber threats," House Permanent Select Committee Intell., Washington, DC, USA, Tech. Rep., 2015.

[34] M. V. Chester and B. Allenby, "Infrastructure as a wicked complex process," *Elementa, Sci. Anthropocene*, vol. 7, no. 1, p. 21, May 2019.

[35] M. Sarwar and T. Rahim Soomro, "Impact of smartphones on society," *Eur. J. Sci. Res.*, vol. 98, no. 2, pp. 216–226, 2013.

[36] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in *Proc. Workshop Future Directions Cyber-Phys. Syst. Secur.*, 2009, vol. 5, no. 1, pp. 1–7.

[37] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," in *Proc. IFIP Int. Fed. Inf. Process., Critical Infrastruct. Protection*, Nov. 2007, pp. 73–82.

[38] T. Rid, "Cyber-sabotage is easy," *Foreign Policy*, to be published.

[39] M. Raggi and D. Schwarz. (Aug. 1, 2019). *LookBack Malware Targets the United States Utilities Sector with Phishing Attacks Impersonating Engineering Licensing Boards*. Accessed: Aug. 6, 2019. [Online]. Available: https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

[40] T. Thomas, "Russia's reflexive control theory and the military," *J. Slavic Mil. Stud.*, vol. 17, no. 2, pp. 237–256, Jun. 2004.

[41] F. King, "Reflexive control and disinformation in putin's wars," Ph.D. dissertation, Colorado State Univ., Fort Collins, CO, USA, 2018.

[42] R. Sprang, "Russia in Ukraine 2013–2016: The application of the new type of warfare maximizing the exploitation of cyber, IO, and media," *Small Wars J.*, to be published.

[43] Department of Homeland Security. (Nov. 20, 2018). *Department of Homeland Security's Cybersecurity and Infrastructure Security Agency*. Accessed: Aug. 6, 2019. [Online]. Available: https://www.dhs.gov/CISA

[44] B. Allenby, "In an age of civilizational conflict," *Jurimetrics*, vol. 56, no. 4, pp. 387–406, 2016.

[45] H. Kissinger, *World Order*. Baltimore, MD, USA: Penguin, 2014.

[46] S. McFate, *The New Rules of War: Victory in the Age of Durable Disorder*. New York, NY, USA: HarperCollins, 2019.

[47] Q. Liang and W. Xiangsui, *Unrestricted Warfare*. Beijing, China: PLA Literature and Arts Publishing House, 1999.

[48] B. Allenby and J. Garreau, "Weaponized narrative: The new battlespace," New Amer. Found./Arizona State Univ. Center Future War, Washington, DC, USA, Tech. Rep., 2017.

[49] P. W. Singer and E. T. Brooking, *LikeWar: The Weaponization of Social Media*. Boston, MA, USA: Houghton Mifflin Harcourt, 2018.

[50] V. Gerasimov, "The value of science is in the foresight," *Mil. Rev.*, to be published.

[51] E. Hutchins, *Cognition in the Wild*. Cambridge, MA, USA: MIT Press, 1995.

[52] W. Shih, *Does Hardware Even Matter Anymore?* Brighton, MA, USA: Harvard Business Review, 2015.

[53] M. Burgess, *Google and Facebook are Gobbling Up the Internet's Subsea Cables*. San Francisco, ca, usa: Wired Magazine, 2018.

[54] C. Bryan-Low, C. Packham, D. Lague, S. Stecklow, and J. Stubbs, "Hobbling Huawei: Inside the U.S. ware on China's tech giant," Reuters, London, U.K., Tech. Rep., May 2019. Accessed: Feb. 6, 2020. [Online]. Available: https://www.reuters.com/investigates/special-report/huawei-usa-campaign/

[55] D. Wang and D. R. Fesenmaier, "Transforming the travel experience: The use of smartphones for travel," in *Proc. Inf. Communication Technol. Tourism*, 2013, pp. 58–69.

[56] X. Hu, Y.-C. Chiu, and J. Shelton, "Development of a behaviorally induced system optimal travel demand management system," *J. Intell. Transp. Syst.*, vol. 21, no. 1, pp. 12–25, Jan. 2017.

[57] S. Kim and B. Coifman, "Comparing INRIX speed data against concurrent loop detector stations over several months," *Transp. Res. C, Emerg. Technol.*, vol. 49, pp. 59–72, Dec. 2014.

[58] Z. Tufekci, "Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency symposium essays," *Colorado Technol. Law J.*, vol. 13, no. 2, pp. 203–218, 2015.

[59] R. Clemlow and G. S. Mishra, "Disruptive transportation: The adoption, utilization, and impacts of ride-hailing in the United States," Univ. California Davis Inst. Transp. Stud., Davis, CA, USA, Tech. Rep. UCD-ITS-RR-17-07, 2017.

[60] P. W. Senge, *The Fifth Discipline: The Art & Practice of The Learning Organization*, New York, NY, USA: Doubleday, 1990.

[61] B. Allenby, "5G, AI, and big data: We're building a new cognitive infrastructure and don't even know it yet," *Bull. At. Scientists*, to be published.

**MIKHAIL V. CHESTER** received the B.S. and M.S. degrees in civil and environmental engineering from Carnegie Mellon University, in 2002 and 2003, respectively, and the M.S. and Ph.D. degrees in civil and environmental engineering from the University of California, Berkeley, in 2005 and 2008, respectively.

He was a Postdoctoral Researcher with the University of California and Lawrence Berkeley National Laboratory, from 2008 and 2011. From 2011 to 2017, he was an Assistant Professor with the School of Sustainable Engineering and the Built Environment, Arizona State University. In 2017, he was promoted to an Associate Professor and founded the Metis Center for Infrastructure and Sustainable Engineering. His research focuses transitioning infrastructure, and its training for the growing complexity and challenges that are emerging in the Anthropocene.

Dr. Chester has twice participated in the National Academy of Engineering's Frontiers program, in 2013 and 2018, and received the American Society of Civil Engineering's Huber Award, in 2017.

**BRADEN R. ALLENBY** graduated from Yale University in 1972. He received the Juris Doctorate from the University of Virginia Law School, in 1978, the master's degree in economics from the University of Virginia, in 1979, and the master's and Ph.D. degrees in environmental sciences from Rutgers University, in Spring 1989 and 1992, respectively.

He is currently the Lincoln Professor of Engineering and Ethics; the President's Professor of Civil, Environmental, and Sustainable Engineering, and of Law; and the Founding Chair of the Consortium for Emerging Technologies, Military Operations and National Security at Arizona State University. From 1995 to 1997, he was the Director of energy and environmental systems with the Lawrence Livermore National Laboratory, and from 1991 to 1992, he was the J. Herbert Hollomon Fellow with The National Academy of Engineering, Washington, DC. He is an AAAS Fellow, a Fellow of the Royal Society for the Arts, Manufactures, and Commerce, and has been a U.S. Naval Academy Stockdale Fellow, from 2009 to 2010.