Chapter 7
Data Science and Resilience

Fred S. Roberts(✉)

DIMACS Center, Rutgers University, Piscataway, NJ 08854, USA
froberts@dimacs.rutgers.edu

Abstract. Our modern digitized socio-technological systems are vulnerable to destructive events such as disease, floods, and terrorist attacks. Data science might help these systems to become more resilient if a variety of challenges described in this paper can be addressed.

Keywords: Resilience · Data science · Disease events · Natural disasters · Terrorism

1 Introduction

Our modern digitized socio-technological systems have enabled dramatic changes in our way of life, but leave us open to destructive events such as diseases, floods, terrorist attacks, and just plain human error. While our systems are vulnerable to such events, the key is how resilient they can become, i.e., how well they are able to recover from disruptions to return to a "normal" state or close to it, and how quickly they can do so. Data science has enabled the digital world of rapid communication, intelligent machines, and instant information. Data science may also hold the key to making our systems more resilient through the availability of massive amounts of data from sensors, satellites, and online activities, allowing us to monitor the state of the power grid, get early warning of emerging diseases, find ways to minimize the effect of flooding, identify looming problems in supply chains, etc. Tools of machine learning can provide early warning of anomalies and alert us that a system may be approaching a critical threshold, thus allowing more time for mitigation that will minimize the effect of disruptions. However, for tools of data science to help us create more resilient systems, we will need to overcome a variety of challenges. It is these challenges we discuss in this paper.

The challenges we present arise in a multitude of applications and the paper will illustrate them to demonstrate the opportunities to enhance resilience. Applications to be discussed include spread of diseases such as COVID-19 and Ebola; natural and man-made disasters such as floods, hurricanes, oil spills, and cyberattacks; counter-terrorism; protecting infrastructure such as the electric power grid and the transportation system; threats to ecosystems, urban systems, food systems, and agriculture; and varied modern challenges arising from climate change, self-driving vehicles, and participatory democracy.

F. S. Roberts and I. A. Sheremet (Eds.): Resilience in the Digital Age, LNCS 12660, pp. 118–138, 2021.
https://doi.org/10.1007/978-3-030-70370-7_7

2 The Fusion Challenge

A key to the data revolution is that massive amounts of data are available from a large number of sources. A key to using data science to enhance resilience is to find effective ways to utilize all those data, to learn from past disruptions, and to get early warning of potential new problems.

Fusion Challenge**:** Many analysis tasks require the fusion of information from numerous media or sources.

2.1 Urban Health and Climate Change

Many key indicators allow us to monitor the overall health of an urban system. These include the state and spatial distribution of critical infrastructure such as the transportation, electricity, gas, and water systems; the capacity of the healthcare system; the distribution of vulnerable populations (such as those living near flood plains or without air conditioning during a heat wave). Many of these indicators are enhanced in importance by climate change.

Climate change affects our urban areas in a multitude of ways. We can expect more and more severe hurricanes, heat waves, drought, and floods. Sea levels will rise. What can urban areas do to prepare for them and mitigate their effects? Fusing data from many sources, can we predict which subways might be flooded? (During "Super Storm" Sandy in 2012, a massive hurricane, some of the subway tunnels in New York City were flooded. Mathematical models developed at Columbia University had predicted exactly which ones [46, 48]. Could we have taken precautionary measures knowing this?) Many power plants are located in low-lying areas near bodies of water. Can we fuse data from many sources to predict which ones might be flooded with sea level rise and move them in advance of those floods or otherwise protect them from flood damage? Train tracks leading to the heart of downtown areas are also often in low-lying areas prone to floods. Can we figure out which tracks are subject to flooding and raise them in advance? The New York City Climate Change Adaptation Task Force set out to address these kinds of questions and, according to a New York City Panel on Climate Change report in 2010, this objective "will require ongoing and consistent monitoring of a set of climate change indicators. Monitoring of key indicators can help to initiate course corrections in adaptation policies and/or changes in timing of their implementation" [47]. Moreover, according to the most recent such Panel on Climate Change report in 2019, "A centralized, coordinated indicators and monitoring system is essential for a comprehensive, city-wide risk assessment of trends in climate and impacts and course correction toward climate change adaptation and resiliency goals and targets" [76].

There are many parameters that determine the normal healthy state of a complex system, and it is necessary to gather information from numerous sources to monitor the health of such a system and get early warning of departures from the "normal." For example, in predicting floods in urban areas, one needs to consider data from rain gauges, radar, satellite algorithms, computer models of atmospheric processes, and hydrological models. In understanding extreme events that may trigger tidal flooding in urban areas, one needs to monitor sea level rise, flood insurance claims from businesses and individuals, urban growth trends, the capacity to restore power after a flood, and socioeconomic factors. Understanding factors involved in previous floods, and using them to get early warning about new floods, can help us mitigate impacts and recover faster. To give just one example, the Peak over Threshold approach uses multiple events to estimate return periods for such floods [60, 82].

Urban heat is a major issue leading to adverse effects not only on public health but also on the economy. Extreme heat events have been a major topic of concern at the US Centers for Disease Control and Prevention for at least a decade [20]. Such events can result in increased incidence of heat stroke, dehydration, cardiac stress, and respiratory distress. Individuals under stress due to climate may also be more susceptible to infectious diseases. Among the data fusion tools designed to determine urban heat exposure for the population in a city is the Spatial and Temporal Adaptive Reflectance Fusion Model (STARFM), using both ground sensor temperature and satellite readings [39, 41]. Fefferman [36] led a study of how to evacuate the most vulnerable individuals to climate controlled environments during a major heat event in an urban area (Newark, New Jersey, US), aimed at minimizing health effects of such an event. Her goal was to determine where to locate evacuation centers and whom to send to which center. The project required a major effort at fusing data as to location of potential centers, travel routes and times to the centers, population size and demographic distribution per city block, and at-risk groups and their likely levels of healthcare required.

2.2 Animal Health: Biodiversity and Farmyards

Biodiversity is the variability in the plant and animal life in species, total numbers of the species, their habitat, and their distribution. Evidence about the health of ecosystems is often obtained by measuring their biodiversity [73]. Identifying species and individual animals or plants offers insight into the crisis of biodiversity loss on our planet. Modern methods of data science allow for the use of a great deal of data to identify species and, sometimes, even individual animals. Identification of individual animals is important if we are trying to estimate the population of a given species in a given region. But how hard is it to identify an individual lion or elephant, especially if we may only see the animal through a "camera trap" image that may only include part of their body and often with poor illumination? Automated methods for identification of species and of individual animals, built on modern methods of artificial intelligence, enable us to get early warning of disruptions to the population of ecosystems. These methods depend upon the fusion of large amounts of biometric data, such as identification of external body pattern, footprints, scent, acoustics, DNA barcoding, etc. [49]. Biometric techniques have the advantage that they don't require invasive interventions since data can be collected without capture, instrumentation or tagging. The amounts of data can be huge. For example, the project called Snapshot Serengeti, based in Tanzania, has collected millions of camera trap images of lions, leopards, cheetahs, elephants, and other animals [63]. Recordings of animal vocalizations can produce over half a gigabyte of data per hour. Machine learning can be very helpful in classifying animal calls. For example, it has been used to classify and count syllables in an animal's call, and can then be used to distinguish between calls of different species, including types of frogs, birds, etc. [86]. We are far from being able to identify species, let alone individual animals, in the wild. However, new methods of artificial intelligence and machine learning are leading to some successes. For instance, [63] describes the use of “deep convolutional neural networks” to identify and count species in the Snapshot Serengeti dataset of 3.2 million images. Identification is accurate 93.8% of the time.

Identification of individual animals is becoming important for domesticated animals. As the number of farms decreases but the number of cattle on each farm grows, it becomes increasingly important to identify individual animals in an efficient way for health monitoring, adjusting feeding to enhance milk production, tracking food and water consumption, and tracking and registration of cattle. Existing methods such as microchip embedding or ear tagging can be expensive and are subject to forgeries or damage. Identification of individual livestock is also important to contain spread of disease and has become recognized as important by international organizations, e.g., in preventing spread of diseases such as Bovine Spongiform Encephalopathy (BSE). Recent work shows that individual cattle can be identified through a deep learning approach based on “primary muzzle point (nose pattern)” characteristics. This addresses the problem of missing or swapped animals (especially during large movements of cattle) and false insurance claims [52, 53]. Tools of face recognition, computer vision, animal behavior, pain metrics, and other tools are already useful in identifying diseases of many domesticated animals, including sheep, and pigs, and to give early warning of potentially devastating epidemics from diseases such as BSE, a critical factor in keeping modern farms resilient [49, 74].

3 The Decision Support Challenge

Decision science is an old subject that was once the domain of social scientists and economists but is now also the domain of computer scientists and mathematicians who, working with traditional decision scientists, are developing tools of modeling, simulation, algorithmics, uncertainty quantification, and consensus. This new data-driven decision support can allow comparison of a vast array of alternative solutions. While using data to make decisions is not new, data science has led to many different techniques to make better decisions, especially new algorithmic approaches. The new field of algorithmic decision theory aims to exploit algorithmic methods to improve the performance of decision makers (human or automated) [15, 67, 71, 79].

Decision Support Challenge: Today’s decision makers have available to them remarkable new technologies, huge amounts of information, and ability to share information at unprecedented speeds and quantities. These tools and resources will enable better decisions if we can surmount concomitant challenges: Data is often incomplete or unreliable or distributed, and involves great uncertainty; many sources of data need to be fused into a good decision, often in a remarkably short time; interoperating/distributed decision makers and decision-making devices need to be coordinated; decisions must be made in dynamic environments based on partial information; there is heightened risk due to extreme consequences of poor decisions; decision makers must understand complex, multidisciplinary problems [71].

3.1 Ebola and COVID-19

The 2014 Ebola outbreak in West Africa should have reminded us that the world is ill-prepared for a severe disease epidemic. When in 2020 the COVID-19 pandemic hit, the world was indeed poorly prepared. The successful fight to contain the Ebola outbreak was helped by application of data analysis and mathematical models to support decision makers. Those models accurately predicted how and where the disease was spreading and how to contain it. The data allowed decision makers to understand things like: how many beds and lab tests would be needed—and where and when to deploy them. Important to the success of the Ebola containment was the sheer and unprecedented magnitude of epidemiological data made available online to researchers and modelers by the World Health Organization and health ministries of the most affected countries. Though modelers had analyzed ongoing epidemics before, such as the 2003 SARS epidemic and 2009 Swine Flu pandemic, they did not have access to such rich sources of data. Data fed into models showed we could stop this outbreak if 70% of Ebola cases could be placed in Ebola treatment units, had effective isolation, and had safe burials [18].

During the COVID-19 pandemic, there has been literally a tsunami of data available within a short time, enabling scientists and policy makers around the world to fit their models and simulations. As models show, faster decisions to shelter in place might have saved a great many lives [66]. However, decision makers have to balance many considerations, which can slow down decisions at potential peril. The more we can develop tools to make effective decisions faster, the better we can ensure resilience in our systems.

3.2 Resilient Supply Chains

During COVID-19, there have been major shortages in items such as ventilators, personal protective equipment and other medical supplies, as well as in consumer goods such as toilet paper and disinfectant wipes and sprays. Our supply chains have been dramatically changed in the digital age, with artificial intelligence allowing both the private sector and the government to minimize inventories due to extremely accurate knowledge of customer demand. However, these AI tools fail when there is an anomalous event. A key to making supply chains more resilient is to develop tools to allow them to identify alternative sources and change priorities in a speedy way [28, 55]. Data science will be critical to support decisions involving changed priorities, alternative suppliers, modified transportation routes or carriers, etc.

3.3 Precision Agriculture

Data science has led to precision agriculture, which allows the farmer to "leverage AI and fine-grain data about the state of crops" to improve yield, helping to make decisions as to when to plant, when to harvest, when to water, when to implement pest control or fertilizer usage, etc. [27]. Thus, using sensors on farm equipment or in the soil can make agricultural practices sustainable and reduce environmental impact through data-driven farming, reducing water and fertilizer use and minimizing the use of pesticides. It can make farms "self-healing" and more resilient. As Daugherty and Wilson [27] observe, "The ultimate goal with precision agriculture is that disparate systems can come together to produce recommendations that farmers can then act on in real time," and of course in the future perhaps even have intelligent machines act on those data without having the farmer in the loop. Being able to modify plans quickly on the basis of data and corresponding models can make agriculture more resilient. However, if watering a field is automated, based on embedded sensors and machine learning, but the crops dry out, entirely new jobs will be needed to recreate what happened in order to improve decision making in the future.

4 The Combinatorial Explosion Challenge

Combinatorial Explosion Challenge: Data science allows comparison of an array of alternative solutions to problems. However, the number of alternatives is often so large that we cannot take all into account in a timely way. We may not even be able to express all possible preferences among alternatives.

4.1 Counterterrorism: Nuclear Detection

Terrorist attacks are a major potential source of disruption to modern societies. One challenge is to minimize the effect of terrorism by doing thorough screening and testing, but designing the most efficient screening protocols can be difficult due to the number of possibilities. Consider inspecting containers at ports for nuclear materials. There are a variety of tests that can be performed on containers, for example determining whether or not the ship's manifest sets off an alarm in an "anomaly detection" program; whether or not the container gives off neutron or Gamma emissions that are above some threshold; whether or not a radiograph image recognition test comes up positive; whether or not an induced fission test comes up positive. One can look at tests sequentially, choosing the next test to perform based on the outcome of the previous test. This kind of sequential diagnosis is common in many fields such as medicine. In container inspection, one can represent the possible tests in a binary decision tree (BDT), where the nodes are tests and we take the right arrow after a given test if the result is positive and left arrow if it is negative. Ultimately, the container is either allowed through or designated for complete unpacking. One seeks a BDT that is optimal in some sense. However, even with five tests, there are 263,515,920 possible BDTs, and the number of possibilities makes it computationally impossible to find an optimal one. Among promising approaches to this problem is specialization of the class of BDTs and development of new search algorithms to move from one tree to better ones [6, 58, 59].

Another example of Combinatorial Explosion also arises from counter-terrorism applications, the problem of comparing the performance of alternative nuclear detection algorithms. The problem is to design experiments to compare algorithm performance, taking into account many relevant factors such as type of special nuclear material being tested, shielding, masking, altitude, humidity, temperature, and speed of vehicle being screened. For each of these factors, there are several possible values, and there are too many combinations to test all of them in experiments. This requires development of tools to design experiments that test together all significant pairs of values [26, 50].

4.2 Testing for Disease: COVID-19

An alternative approach to the container inspection problem is a tool called SNSRTREE [12, 13]. This tool involves a large-scale linear programming model for sequential inspection of containers that allows for mixed strategies, accommodates realistic limitations on budget and testing capacity and time limits, and is computationally more tractable. Recently, research has begun on applying this tool to testing for COVID-19. The goal is to determine how to optimally select from among the available tests for COVID-19 according to the person, their work, the results of any prior tests, and current, dynamic test availability. The goal is to use SNSRTREE to determine the probability that a specific individual is, or is not, "infective." Tests for the COVID-19 infection include self-reports of symptoms, thermometer readings, clinical observations, nasal swab tests, saliva tests, etc. Tests vary as to cost, reliability, and assay time to get a result. To develop optimal testing policies, we first ask for the result of a first test, and depending on that result, we may reach a decision or choose a second test. After a second test, we may reach a decision, or choose a third test, etc. Every such policy has a cost, integrating the expected cost of the tests with the economic and human costs of false positives and false negatives. SNSRTREE finds the entire set of "optimal" testing policies for all possible budgets. Read in one way, it provides least estimated infection at a given cost; read the other way, it provides lowest estimated cost for a given infection control. What makes the modification of SNSRTREE or any other algorithm for application to COVID-19 testing complicated is that infection is a moving (time dependent) target rather than a fixed property; tests may have different assay times and availabilities over time; and test results may not be stochastically independent – all of which add to the combinatorial explosion of possibilities.[1]

4.3 Ecological Monitoring

Still another example of the Combinatorial Explosion Challenge comes from NEON (National Ecological Observatory Network), a project that involves gathering data from 20 sites across the US to get a continent-wide picture of the impacts on natural resources and biodiversity of climate change, land use change, and invasive species. The understanding gained from NEON can contribute to the resilience of the ecosystem in numerous ways. How are those 20 sites chosen? NEON divides the country into 8 million patches. For each patch, the project collects 9 pieces of information about its ecology and climate, clusters the patches, and chooses a representative patch for each cluster. But why limit this to 9 pieces of information when one could easily come up with 100 pieces of information about each patch? The problem is that it would then become combinatorially impossible to do the clustering [23].

[1] Thanks to Endre Boros, Dennis Egan, Nina Fefferman, Paul Kantor, and Vladimir Menkov for discussions and the specific ideas in this paragraph.

5 The Real-Time Analytics Challenge

Near-real-time situational awareness (real-time analytics) is becoming increasingly feasible, based on massive amounts of data from simulation and modeling, mobile applications, and sensors. Such data can be too rapid for real-time human consumption or exploration.

Real-Time Analytics Challenge: Some data rates are so large that not all the data can be saved and yet real-time or almost real-time decisions must be made.

5.1 Resilience in the Electric Power Grid

The electric power grid provides an example where real-time analytics can dramatically improve resilience.[2] Today's electric power systems operate under considerable uncertainty. Cascading failures can have dramatic consequences [3]. Algorithmic methods are needed to improve security of the energy system in light of its haphazard construction and dynamically changing character and to find early warning of a changed state, i.e., to rapidly detect anomalies. "Smart grid" data sources enable real-time precision in operations and control previously unobtainable (see e.g., [2, 4, 5, 23, 25, 88]): Time-synchronous phasor data, linked with advanced computation and visualization, will enable advances in state estimation, real-time contingency analysis, and real-time monitoring of dynamic (oscillatory) behaviors in the system; sensing and measurement technologies will support faster and more accurate response, e.g., through remote monitoring; advanced control methods will enable rapid diagnosis and precise solutions appropriate to an "event." Status updates that used to come in every two to four seconds are now approaching ten times a second using new phasor technologies. That rate may be too rapid for a human alone to absorb the presence of an anomaly in time to act upon the information, thereby requiring software agent or algorithmic support.

5.2 Smart Transportation Systems

Traffic management in "smart cities" presents many examples of the Real-time Analytics Challenge.[3] "Intelligent transportation systems" involve integrated fare management, variable road usage charging, and traffic information made available in real time, all requiring fusion of a great deal of information. Real-time traffic management takes account of sensors of all kinds, ability to monitor the actual traffic situation (volumes, speeds, incidents), and the ability to control or influence the flow using that information to reduce traffic congestion, deal with incidents, and provide accurate information to drivers and authorities. Sensor data depends heavily on GPS data that needs to be related to the underlying network by map matching algorithms that are computationally

[2] Much of the following discussion is based on a white paper [1] in [23] and a presentation by Gilbert Bindewald of the US Department of Energy to the SIAM Science Policy Committee on October 28, 2009.

[3] Many of the ideas on traffic management here are taken from the talk "Smart Cities – How can Data Mining and Optimization Shape Future Cities," by Francesco Calabrese of IBM Ireland, at the DIMACS/LAMSADE workshop on Smart Cities, Paris, Sept. 2011.

expensive. GPS data is sampled at irregular intervals, possibly with large gaps – which requires advanced analytics to reconstruct GPS trajectories. Also, GPS data is inaccurate, needs "cleaning." Additional complexity arises from the need to combine the "hard" numerical readings of sensors monitoring vehicle movements with the "soft" natural language utterances of drivers and tweets of the public. Understanding human transit demands/needs in real-time involves challenges to help design adaptive urban transportation systems, help citizens navigate the city, detect and predict travel demand, and offer real-time alternative routings in case of problems. The ability to offer such real-time adjustments can make today's smart transportation systems more resilient. For some relevant references, see [8, 40].

5.3 Food Security

The food system has multiple components: producers of food, those who process, ship, or sell food products, and those who shop for food and consume it. At all steps "from farm to fork" there are possible disruptions [83]. Such disruptions include extreme weather events, animal diseases, terrorist attacks, and disease events such as COVID-19, which has both closed down meat packing plants, leading to shortages, and rapidly changed demand, leading to farmers plowing under crops and pouring out milk. Today's sensing and computing capacities allow us to monitor the food system in real time and to take action to maintain security of the food supply. Such monitoring includes observational data (soil conditions, land use) and data on social processes and preferences. Automatic image processing of satellite data [56], information from crop and soil sensors, and real-time reports of changing supply chain conditions, can be used to gain real-time awareness and make changes. Such methods have been used for example to estimate the resilience of the wheat market to potential ruptures in the global transportation system [34]. For more on real-time monitoring of the food system, see [51][4].

5.4 Resilient Ecosystems

Ecosystems are subject to increasing disturbances in the face of global change (climate change, land use change, migration patterns, increasing urbanization, etc.). Resilience of ecosystems allows them to bounce back from perturbations [85]. Is it possible to judge in real-time when an ecosystem is at the brink of suffering a perturbation that would irreversibly disrupt it, i.e., when it is on the edge of collapse [9, 11]? Examples of such dramatic "state changes" in an ecosystem are desertification of certain parts of the earth [21, 33], coral bleaching [10], lake eutrophication [16], major disruption of the atmospheric chemistry as a result of agriculture [38], and the transformation of tropical forests under slash and burn agriculture [54]. One approach is to study satellite images over a long period of time (many years) and use "deep learning" methods to identify ecosystems that are stressed and that might have undergone a shift from a stable state to another. By identifying general characteristics of an ecosystem including climate fluctuations, biogeochemical cycles or vegetation-atmosphere interactions, it may be possible to identify those characteristics that indicate a shift is about to occur.[5]

[4] Thanks to Hans Kaper for many of the ideas in this paragraph.

[5] Many of the ideas in this paragraph are due to Paolo D'Odorico and Wayne Getz.

6 The Vulnerabilities Challenge

Modern society is critically dependent upon data from manufacturing and production systems, power and water, transportation, financial transactions, medicine, etc. Vulnerabilities are ever present, enhancing cyberattacks on our infrastructure, causing cascading failures, leading to rapid spread of anomalies and exacerbating the impacts of all kinds of failures. It is the very ability to utilize and benefit from large amounts of data that sometimes creates vulnerabilities.

Vulnerabilities Challenge: How do we identify new vulnerabilities caused by usage of data? How do we develop tools for monitoring and minimizing such vulnerabilities?

6.1 Medical Facilities

Electronic medical records are a case in point. They lead to being able to share data about a person's medical condition rapidly and with a variety of medical personnel. However, these electronic medical records lead to vulnerabilities. Recently several hospitals have had to postpone surgeries after having lost access to electronic medical records in a cyberattack, and had to pay ransom to regain access to these records [61]. During times of uncertainty and confusion, especially disasters, criminals take full advantage. That is particularly true of the COVID-19 pandemic. An FBI release says that criminals are "using COVID-19 as a lure to deploy ransomware … designed to lock" hospital or public health department computers [35]. There have already been examples of ransomware attacks on hospitals and labs treating COVID-19 patients or working on treatments, vaccines, etc. [37]. Numerous other frauds and scams by criminals during the COVID-19 pandemic also seek to take advantage of the situation. The FBI release describes offers of sham treatments and vaccines, bogus investment opportunities in medical companies, and people impersonating doctors demanding payment for treatment.

6.2 Cybersecurity of Supply Chains

Information and communication devices have enabled rapid information sharing, created the ability to make financial transactions from anywhere, and provided access from the workplace to markets worldwide. However, the very nature of these devices as tools, which use, process and share huge amounts of data rapidly, has led to vulnerabilities. In recent years, there has been a major concern about cyber threats to information and communication devices and processes. A report of the US Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force [22] gives a great deal of detail about the importance of and new approaches to supply chain risk assessment in the information and communication technology (ICT) domain, as do reports from the US National Institute of Standards and Technology (NIST) [14] and the US National Counterintelligence and Security Center, Supply Chain Directorate [62]. The CISA report makes it clear that cyber is a key issue. As a supply chain is only as strong as its weakest link, all components of the supply chain have to be engaged in cybersecurity issues, but how to achieve this goal is a major challenge. A disruption in one device connected to the supply chain can cascade through the entire system, and the development of protection against such cascading effects of cyberattacks is of central importance. The maritime transportation system is key to the world's supply chains. See Rose [75] for some work on models of cascading impacts of cyberattacks on the maritime transportation system. Some of those cascading effects on supply chains result from supply substitutions. How can the potential for supply substitutions to lead to cascading failures be minimized? Models such as those of [31, 32] of how to control the cascading impact of power grid disruptions are very relevant here, and could lead to improved resilience of many types of supply chains.

6.3 Autonomous Vehicles

Due to the ready availability of data, there is a huge increase in number of cyber-physical systems. Today's cars are more like computers on wheels. Yet, the very ability to utilize large amounts of data to perform better leads to vulnerabilities. Cyber-physical systems control much of how a car operates. This makes today's cars already semiautonomous, taking decisions away from the driver, and thereby frequently aiding in preventing accidents. But could a criminal or terrorist take control of a car remotely through a cyberattack and use it to cause damage? This seems to be a serious challenge as in-car technology becomes more sophisticated. And it is likely to become even more of a challenge as we develop fully autonomous vehicles. In 2013, Miller (Twitter) and Valasek (IOActive) demonstrated they could take control of a Toyota Prius and a Ford Escape from a laptop [42]. They were able to remotely control the smart steering, braking, displays, acceleration, engine, horn, lights, and so on. As we move to self-driving cars, similar vulnerabilities might exist. This is not just hypothetical. Already in our seaports, trucks and cranes operate in driverless mode, and there have been cyberattacks on cranes in ports [29, 30]. One approach to minimizing the impact of attacks on self-driving cars begins with risk assessment of different kinds of attacks. See [72] for an approach.

6.4 Oil Rigs

The failure of a blowout preventer on an oil rig in the Gulf of Mexico in 2010 led to the devastating Deepwater Horizon oil spill, the largest oil spill in US history. That was not due to a cyberattack. However, there have been cyberattacks on oil rigs. According to security company ThetaRay, a cyberattack on a floating oil rig off the coast of Africa managed to tilt the rig slightly and as a result it was forced to shut down. It took a week to identify and fix the problem [87]. In another drilling rig event, in 2010, a drilling rig being moved at sea from South Korea to South America was infected by malicious software. Its critical control systems could not operate and it took 19 days to fix matters [24, 87]. The cyberattack infected the computers controlling the blowout preventer, the system at fault for the Deepwater Horizon accident. The results could have been disastrous. Oil rigs are critically dependent on GPS for stability, yet hackers have been able to tilt an oil rig, putting it out of commission for days at high cost. Modern GPS, dynamic positioning systems, and other technologies that depend on large amounts of data have made it possible to manipulate oil rigs in efficient ways, yet open them up to attacks and outages [29]. How can we minimize the impact of such attacks? That will be crucial to make oil rigs and other systems more resilient.

7 The Information Sharing Challenge

Secure information sharing is a key to enable organizations and individuals to work together on a wide range of issues. Such information sharing is a critical component of ensuring resilience of systems and networks.

Information Sharing Challenge: Information sharing requires appropriately safeguarding both systems and information; selecting the most trusted information sources; and maintaining secure systems in potentially hostile settings. How can one best accomplish these things?

7.1 The Terror Attacks of September 11, 2001

Failure to detect and prevent the September 11th, 2001 attacks in New York City was, in many ways, a result of an intelligence failure due to lack of information sharing. At the time, there was no coordinated way to "connect the dots." Subsequent analyses, detailed in the Report of the National Commission on Terrorist Attacks Upon the United States, also known as the 9/11 Commission Report [84], resulted in an emphasis on information sharing to facilitate situational awareness and understanding. In addition to the loss of life, the 9/11 attacks had a major economic impact in the US, in particular on the transportation system, from which it took a long time to recover. The hope is that information sharing will prevent successful terrorist attacks or criminal behavior, or at least minimize their impacts, i.e., make the country and its various systems more resilient.

In order to gain situational understanding when there are many organizations or individuals each having some relevant information, one can create an 'information sharing environment' (ISE) - a decentralized, distributed, coordinated milieu that connects existing systems and builds on their capabilities, while protecting individuals' privacy [19]. In the US, for example, "fusion centers" were created to share information among numerous agencies and the private sector following the September 11th attacks. They can have thousands of federal, state and local partners, and utilize information from numerous government agencies and the private sector, to aid in counter-terrorism and anti-crime efforts. Successful creation of an ISE requires implementation of both technical and operational components. Technical components (like interoperability and rules as to who can gain access and how) are necessary, but also fundamental are the human components and procedures that ultimately allow an ISE to succeed. An ISE requires coordination and integration of information-sharing through collaboration and cooperation. However, there have to be shared standards for identification, access, and utilization of information, there have to be policy, procedures, and technical solutions for safeguarding information, and there need to be standards and accountability procedures for the protection of privacy, civil rights, and civil liberties.

7.2 "Participatory Democracy"

Information sharing is coming to be a key component of what some people are calling "participatory democracy." Here, the idea is that participation by all stakeholders, including the public, can lead to better policies for governments. While the concept of participatory democracy goes back to Athenian days [7] it is becoming more and more important in this digital age. The book [70] develops the concept of "e-democracy," which, among other things, includes web-based participation leading to changes in public policy. The underlying assumption is that decisions reached through public participation can lead to more stable societies, smarter cities, etc. Such participatory democracy has been explored in the context of water usage, power supply, health care, and other applications, but it requires the development of methods of sharing information and views, beliefs, and preferences. Tools for reaching good decisions using participatory methods have been explored by various authors, for example [69]. The goal is to develop tools to facilitate stakeholders' participation and achieve collective commitment, which in turn would seem to lead to greater stability and resilience.

7.3 "Super Storm" Sandy

After "Super Storm" Sandy, the massive hurricane that hit New York City in 2012, the port of New York/New Jersey was left dramatically damaged. Yet, it was very resilient and recovered quickly. In a report on the resilience of the port [81], the authors point out that "soft" resilience strategies were vital in its recovery after Hurricane Sandy. Such strategies "include ways to reduce vulnerability and improve response and recovery capability through planning, people, partnerships and policy" and "planning for response and recovery; increasing access to high quality data; and developing a web of bonds, ties and relationships across sectors - that is, building what scholars have called 'social capital' through collaboration." Thus, a stronger social infrastructure (keyed by good information sharing) led to a more resilient port.

7.4 Secure Multi-party Computation

One theoretical approach of note has come to be called "Secure Multiparty Computation" [89], an area aiming at allowing parties to jointly compute something over their inputs while keeping those inputs private. It is a model for "secure information sharing." We have begun to see a new effort in systematizing secure computation to allow decision makers to understand essential strengths and weaknesses of different secure computation solutions (e.g., whether or not they guarantee fairness and their prerequisites regarding correctness, auditability, and compliance) and determine which best applies in a given scenario [68].

8 The Trustworthiness Challenge

Data comes from multiple sources and some are more accurate than others. Multiple information sources often provide inconsistent or conflicting information – whether maliciously, or due to noise. This is especially so in emergency situations where heterogeneous information streams describe damage, physical needs, information needs, etc. in different locations. To utilize the vast amounts of data available to us in this age of Big Data, we have to understand what sources we can trust. We need precise definitions of factors contributing to trustworthiness: accuracy, completeness, bias. For work along these lines, see for example [64, 65]. Work is also needed to develop claim verification systems, with automated claim verification by finding supporting and opposing evidence.

The Trustworthiness Challenge: How can we develop computational frameworks and other tools that address the problem of trustworthiness in disasters and other situations?

8.1 Trust in Authorities During Disasters

Responses to disasters will work better if people trust those in charge and comply with instructions, thus allowing more rapid and effective response to disasters and making society more resilient. Greenberg [44] argues that there are two factors that determine whether individuals trust organizations, in particular government organizations. One is perception of the competence of the organization and the second is the perception that the organization possesses values and intentions consistent with those of the individual asked to trust it, things like fairness or non-bias or willingness to listen and communicate. In 2013, after Super Storm Sandy, Greenberg [43, 44] investigated the New Jersey public's willingness to support rebuilding of devastated parts of the state. He asked residents if they were willing to contribute to a special fund for rebuilding. "The vast majority were unwilling, and we found that mistrust of the state was a strong predictor of their unwillingness to contribute. Many did not trust state government to use a dedicated fund for the designated purpose" [44]. In the midst of a disaster such as the COVID-19 pandemic, many technologies are being touted as helpful, e.g., for screening, testing, contact tracing, enforcing social distancing, etc. If Greenberg is right, issues of fairness and ethics involving the government agencies that will deploy the technologies will enter just as significantly as issues of technical competence of those agencies and technical performance of the technologies.

8.2 Risk Communication and Human Perception During a Pandemic

COVID-19 reminded us that communications and human behavior are important factors to consider when preparing for and during a disaster, e.g., a pandemic. How does human behavior such as panic hoarding of toilet paper, hand sanitizer, and pasta, which we have seen during the COVID-19 pandemic, arise? To some extent, hoarding is a rational response to being told not to venture out a lot, in which case it makes sense to stock up on a lot of goods when you do [57]. How do communications impact hoarding behavior? Among other things, they can impact our trust in the supply system. In the US, there were some early inconsistencies in such messaging. For example, the Centers for Disease Control and Prevention recommended keeping a 2-week supply of food at hand and the Federal Drug Administration recommended that people should only buy enough for the week ahead [57]. Good risk communication is a key to resilience in the case of a disaster.

One critical element involved in reopening an economy after people are required to stay home at the height of a disease outbreak such as COVID-19 is the availability of healthy and willing workers. It is important to understand the workers' mental models of the risk of infection, and how they frame decisions related to the safety of the workplace. This will involve questions relating to workers' concerns about competence of those laying out guidelines about workplace safety. For relevant research on how workers might make such decisions after disasters, see [77, 78], where the authors studied flu epidemics and an urban biological catastrophe involving anthrax and explored people's decisions about returning to work. Their work demonstrates the importance of risk communication in making the economy more resilient.

8.3 Identity and Access Management

To return to the topic of information sharing discussed in Sect. 7, another critical principle underlying a successful information sharing environment (ISE) is trust. This is both a human and a technical issue. ISEs only work when, over time, participants learn to work together and trust each other. On the technical side, trust can be accomplished through identity credential access management solutions, which are a means for participants to have confidence in the identity of collaborators. "Trustmarks" are digitally-signed assertions by a third party assessor that are shared between parties seeking to share information. The parties treat a third party verification as evidence that the trustmark recipient meets the trust and requirements as set forth in some agreement. For more information on trustmarks, see [45]. For more on the subject that is coming to be called identity and access management, see [80].

Proving your identity is part of information sharing. Proving that you have the authority to do something is another component of identity and access management [17], and this subject can play a role in enhancing recovery during a disaster. Consider a firefighter from New Jersey who goes to Florida to help in the recovery from a hurricane, an emergency management technician from New Jersey who goes to California to help treat earthquake victims, or a policeman from New Jersey who goes to New York City to help control a terrorist standoff. How can these people convince the responsible people at the disaster scene that they are who they are, but more importantly that they have official credentials such as a security clearance or a permit to carry a weapon or a hazardous materials cleanup certificate? The tools of identity and access management can enable their smart phones to carry encrypted information about their credentials that will speed up the approval for their involvement by the local authorities [17]. This is an important, growing field that will help enhance trust and as a result enhance resilience in disaster situations.

9 Closing Comments

Today's world of big data, massive computing capacity, artificial intelligence, and machine learning makes it possible to learn how to build resilience into systems. The deluge of data from in-situ sensors, remote sensing, images, videos, recordings, makes it possible to observe changes in systems across temporal and spatial scales. These same sources of data should make it possible to develop tools for characterizing resilience. However, in addition to the challenges discussed in this paper, another critical one is that there are no agreed-upon metrics to measure whether a system has become more (or less) resilient, or many tools for improving a system's resilience.

As we have observed, resilience of a system can be enhanced by learning from the past to sense emerging risks. As more data becomes available, this learning can benefit. We can fuse massive amounts of data of different kinds, combining with machine learning tools for anomaly detection, to provide early warning that a system might be in danger. By providing tools for faster awareness of problems, data science can give systems time to take mitigating actions. This learning can only be useful, however, if we can identify appropriate features and indicators, determine how to measure them, and use them as input into tools of data science to learn which parameter configurations allow a system to recover to a healthy state if it has been disrupted.

Acknowledgement. The author thanks the National Science Foundation for support under grants DMS-1737857 and CCF-1934924 to Rutgers University.

References

1. Adem, A., et al.: Human well-being and the natural environment Appendix 1. In: Cozzens, M., Roberts, F.S. (eds.) Mathematical and Statistical Challenges for Sustainability, pp. 61–85. American Mathematical Society, Providence (2011)
2. Amin, M.: Powering the 21st century: we can - and must - modernize the grid. IEEE Power Energ. Mag. **3**, 93–95 (2005)
3. Amin, M., Schewe, P.: Preventing blackouts. Sci. Am. **296**, 60–67 (2007)
4. Amin, M., Stringer, J.: The electric power grid: today and tomorrow. Mater. Res. Soc. Bull. **33**, 399–407 (2008)
5. Amin, M., Wollenberg, B.: Towards a smart grid. IEEE Power Energ. Mag. **3**, 34–41 (2005)
6. Anand, S., Madigan, D., Mammone, R., Pathak, S., Roberts, F.: Experimental analysis of sequential decision making algorithms for port of entry inspection procedures. In: Mehrotra, S., Zeng, D.D., Chen, H., Thuraisingham, B., Wang, F.-Y. (eds.) ISI 2006. LNCS, vol. 3975, pp. 319–330. Springer, Heidelberg (2006). https://doi.org/10.1007/11760146_28
7. Arenilla, M.: Concepts in democratic theory. In: Rios Insua, D., French, S. (eds.) e-Democracy, pp. 15-30. Springer, Dordrecht (2010). https://doi.org/10.1007/978-90-481-9045-4_2
8. Baptista, A.T., Bouillet, E., Calabrese, F., Verscheure, O.: Towards building an uncertainty-aware personal journey planner. In: Proceedings 14th International IEEE Conference on Intelligent Transportation Systems (ITSC), pp. 378–383. IEEE (2011). https://doi.org/10.1109/ITSC.2011.6082962.
9. Barnosky, A.D., et al.: Approaching a state shift in earth's biosphere. Nature **486**, 51 (2012)
10. Bellwood, D.R., Hughes, T.P., Folke, C., Nystrom, M.: Confronting the coral reef crisis. Nature **429**, 827–833 (2004). https://doi.org/10.1038/nature02691
11. Boettiger, C., Hastings, A.: Early warning signals and the prosecutor's fallacy. Proc. R. Soc. Lond. B Biol. Sci. **279**, 4734–4739 (2012)
12. Boros, E., Fedzhora, L., Kantor, P.B., Saeger, K., Stroud, P.: A large-scale linear programming model for finding optimal container inspection strategies. Naval Res. Logist. (NRL) **56**(5), 404–420 (2009). https://doi.org/10.1002/nav.20349

13. Boros, E., Fedzhora, L., Kantor, P.B., Saeger, K., Stroud, P.: Large scale LP model for finding optimal container inspection strategies. Technical report RUTCOR 26–2006. Rutgers University Center for Operations Research (2006)
14. Boyens, J., Paulsen, C., Moorthy, R., Bartol, N.: Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST Special Publication 800-161, April 2015. https://www.dni.gov/files/NCSC/documents/supplychain/20190327-NIST-Sp-800-161.pdf. Accessed 14 Jan 2020
15. Brafman, R.I., Roberts, F.S., Tsoukiàs, A. (eds.): ADT 2011. LNCS (LNAI), vol. 6992. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-24873-3
16. Carpenter, S.R., et al.: Early warnings of regime shifts: a whole-ecosystem experiment. Science **332**, 1079–1082 (2011). https://doi.org/10.1126/science.1203672
17. CCICADA: CCICADA launches ID verification project to speed responses to natural and terrorist disasters. CCICADA Center, Rutgers University, 22 March 2016. https://ccicada.org/2016/03/22/ccicada-launches-id-verification-project-to-speed-responses-to-natural-and-terrorist-disasters/. Accessed 2 June 2020
18. CCICADA: Fight against Zika virus to benefit from Ebola math models. CCICADA Center, Rutgers University, 5 May 2016. https://ccicada.org/2016/05/05/fight-against-zika-virus-to-benefit-from-ebola-math-models/. Accessed 1 June 2020
19. CCICADA: Expanding information-sharing environments to fight crime and terror is goal of Rutgers research team. CCICADA Center, Rutgers University, 6 April 2017. https://ccicada.org/2017/04/06/expanding-information-sharing-environments-to-fight-crime-and-terror-is-goal-of-rutgers-research-team/. Accessed 31 May 2020
20. Centers for Disease Control and Prevention, National Center for Environmental Health: Extreme Heat Events. https://www.cdc.gov/climateandhealth/pubs/ClimateChangeandExtremeHeatEvents.pdf. Accessed 1 June 2020
21. Cherlet, M., Hutchinson, C., Reynolds, J., Hill, J., von Sommer, S., Maltitz, G.: World Atlas of Desertification. Publication Office of the European Union, Luxembourg (2018)
22. CISA: Cybersecurity and Infrastructure Security Agency Information and Communications Technology Supply Chain Risk Management Task Force: Interim report: status update on activities and objectives of the task force, September 2019. https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf. Accessed 14 Jan 2020
23. Cozzens, M.B., Roberts, F.S. (eds.): Mathematical and Statistical Challenges for Sustainability. American Mathematical Society, Providence (2011)
24. CyberKeel: Maritime cyber-risks: Virtual pirates at large on the cyber seas. White Paper, CyberKeel, Copenhagen, 15 October 2014
25. Daki, H., El Hannani, A., Aqqal, A., Haidine, A., Dahbi, A.: Big Data management in smart grid: concepts, requirements and implementation. J. Big Data **4**(1), 1–19 (2017). https://doi.org/10.1186/s40537-017-0070-y
26. Dalal, S.R., Jain, A., Kantor, P.B.: Creating configurations for testing radiation portal algorithms using factor covering combinatorial designs. Presented at the 2015 IEEE International Symposium on Technologies for Homeland Security, Boston, MA (2015)
27. Daugherty, P.R., Wilson, H.J.: Human + Machine: Reimagining Work in the Age of AI. Harvard Business Review Press, Boston (2018)
28. Deloitte: COVID-19: Managing supply chain risk and disruption. Coronavirus highlights the need to transform traditional supply chain models (2020). https://www2.deloitte.com/global/en/pages/risk/articles/covid-19-managing-supply-chain-risk-and-disruption.html. Accessed 28 Apr 2020
29. DiRenzo III, J., Goward, D.A., Roberts, F.S.: The little known challenge of maritime cyber security. In: Proceedings 6th International Conference on Information, Intelligence, Systems, and Applications (IISA), pp. 1–5. IEEE, Piscataway (2015)

30. DiRenzo, J., III., Drumhiller, N., Roberts, F.S. (eds.): Issues in Maritime Cyber Security. Westphalia Press, Washington, DC (2017)
31. Dobson, I., Carreras, B.A., Lynch, V.E., Newman, D.E.: Complex systems analysis of series of blackouts: cascading failure, critical points, self-organization. Chaos **17**, 026103 (2007). https://doi.org/10.1063/1.2737822
32. Dobson, I., Carreras, B.A., Newman, D.E.: A loading-dependent model of probabilistic cascading failure. Prob. Eng. Inf. Sci. **19**(1), 15–32 (2005)
33. D'Odorico, P., Bhattachan, A., Davis, K.F., Ravi, S., Runyan, C.W.: Global desertification: drivers and feedbacks. Adv. Water Res. **51**, 326–344 (2013)
34. Fair, K.R., Bauch, C.T., Anand, M.: Dynamics of the global wheat trade network and resilience to shocks. Sci. Rep. **7**, 7177 (2017)
35. FBI: FBI and Secret Service working against COVID-19 threats. FBI National Press Office, 15 April 2020. https://www.fbi.gov/news/pressrel/press-releases/fbi-and-secret-service-working-against-covid-19-threats. Accessed 30 Apr 2020. (A version of this appeared in the Washington Post online edition of 14 April 2020.)
36. Fefferman, N., Emergency shelter location and resource allocation. In: Lacy, C. (ed.), Report on the Development of the University Center for Disaster Preparedness and Emergency Response (UCDPER), pp. 50–86. Rutgers University, New Brunswick (2011). https://www.researchgate.net/publication/279336405_Development_of_the_University_Center_for_Disaster_Preparedness_and_Emergency_Response_UCDPER. Accessed 2 June 2020.
37. Gallagher, R., Bloomberg News: Hackers "without conscience" demand ransom from dozens of hospitals and labs working on coronavirus. Fortune, 1 April 2020. https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus/. Accessed 31 May 2020
38. Galloway, J.N., et al.: The nitrogen cascade. AIBS Bull. **53**(4), 341–356 (2003)
39. Gao, F., Masek, J., Schwaller, M., Hall, F.: On the blending of the Landsat and MODIS surface reflectance: predicting daily Landsat surface reflectance. IEEE Trans. Geosci. Remote Sens. **44**(8), 2207–2218 (2006)
40. Gasparini, L., Bouillet, E., Calabrese, F., Verscheure, O., O'Brien, B., O'Donnell, M.: System and analytics for continuously assessing transport systems from sparse and noisy observations: case study in Dublin. In: Proceedings of IEEE Conference on Intelligent Transportation Systems, pp. 1827–1832. IEEE (2011)
41. Gevaert, C.M., García-Haro, F.J.: A comparison of STARFM and an unmixing-based algorithm for Landsat and MODIS data fusion. Remote Sens. Environ. **156**, 34–44 (2015)
42. Greenberg, A.: Hackers reveal nasty new car attacks – with me behind the wheel. Forbes, 12 August 2013. https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#3fe5a27c228c. Accessed 31 May 2020
43. Greenberg M.: Willingness to pay for a sustainable shoreline: public reactions follow Super-storm Sandy in New Jersey, USA. In: Krope, J., Olabi, A.G., Goricanec, D. (eds.) Sustainable Energy and Environmental Protection, SEEP, Maribor, Slovenia, pp. 46–50 (2013)
44. Greenberg, M.R.: Energy policy and research: the underappreciation of trust. Energy Res. Soc. Sci. **1**, 152–160 (2014)
45. GTRI: GTRI NSTIC Trustmark Pilot. https://trustmark.gtri.gatech.edu/technical-framework/. Accessed 31 May 2020
46. Hood, P.: Sandy's wake. Columbia Magazine, Winter 2012–2013. https://magazine.columbia.edu/article/sandys-wake. Accessed 2 June 2020.
47. Jacob, K., Blake, R.: Indicators and monitoring. In: Climate Change Adaptation in New York City: Building a Risk Management Response. The New York City Panel on Climate Change 2010 Report. Annals of The New York Academy of Sciences, Chapter 7, vol. 1196, pp. 1–354 (2010)

48. Jacob, K., et al. (eds.): Responding to climate change in New York State: the ClimAID integrated assessment for effective climate change adaptation in New York State, pp. 299–369. Technical report 11-18, New York State Energy Research and Development Authority (2011)
49. Jewell, Z.C., et al.: Automated biometrics for biodiversity assessment: opportunities and challenges (2020, in preparation)
50. Kantor, P., Dalal, S., Jain, A., Nelson, C.: Optimal selection of configurations to test radiation detectors. Presented at the Informs Annual Meeting, San Francisco, CA (2014)
51. Kaper, H.G., Engler, H.: Modeling food systems. In: Kaper, H.G., Roberts, F.S. (eds.) Mathematics of Planet Earth: Protecting Our Planet, Learning from the Past, Safeguarding for the Future, pp. 267–296. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-22044-0_10
52. Kumar, S., et al.: Deep learning framework for recognition of cattle using muzzle point image pattern. Measurement **116**, 1–17 (2018)
53. Kumar, S., Singh, S.K., Singh, R.K, Singh, A.K.: Muzzle point pattern-based techniques for individual cattle identification. In: Kumar, S., Singh, S.K., Singh, R.K., Singh, A.K (eds.) Animal Biometrics: Techniques and Applications, pp. 111–135. Springer, Singapore (2017)
54. Lawrence, D., D'Odorico, P., Diekmann, L., DeLonge, M., Das, R., Eaton, J.: Ecological feedbacks following deforestation create the potential for a catastrophic ecosystem shift in tropical dry forest. Proc. Natl. Acad. Sci. U.S.A. **104**(52), 20696–20701 (2007)
55. Liao, R., Fan, Z.: Supply chains have been upended. Here's how to make them more resilient. World Economic Forum, 6 Apr 2020. https://www.weforum.org/agenda/2020/04/supply-chains-resilient-covid-19/. Accessed 28 Apr 2020
56. Lobell, D.B.: The use of satellite data for crop yield gap analysis. Field Crops Res. **143**, 56–64 (2013)
57. Lundstrom, M.: Hoarding in a pandemic: a problem of messaging, selfishness, or simply fear? FairWarning, 21 March 2020. https://www.salon.com/2020/03/21/hoarding-in-a-pandemic-a-problem-of-messaging-selfishness-or-simply-fear_partner/. Accessed 30 Apr 2020
58. Madigan, D., Mittal, S., Roberts, F.S.: Sequential decision making algorithms for port of entry inspection: overcoming computational challenges. In: Muresan, G., Altiok, T., Melamed, B., Zeng, D. (eds.) Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI-2007), pp. 1–7. IEEE Press, Piscataway (2007)
59. Madigan, D., Mittal, S., Roberts, F.S.: Efficient sequential decision-making algorithms for container inspection operations. Naval Res. Logist. **58**, 637–654 (2011)
60. Méndez, F.J., Menéndez, M., Luceño, A., Losada, I.J.: Estimation of the long-term variability of extreme significant wave height using a time-dependent peak over threshold (POT) model. J. Geophy. Res. Oceans **111**(C7) (2006)
61. Mohney, G.: Hospitals remain key targets as ransomware attacks expected to increase. ABC News, 15 May 2017. https://abcnews.go.com/Health/hospitals-remain-key-targets-ransomware-attacks-expected-increase/story?id=47416989. Accessed 1 June 2020.
62. National Counterintelligence and Security Center, Supply Chain Directorate: Supply Chain Risk Management: Best Practices. https://www.dni.gov/files/NCSC/documents/supplychain/20190405-UpdatedSCRM-Best-Practices.pdf. Accessed 14 Jan 2020
63. Norouzzadeh, M.S., et al.: Automatically identifying, counting, and describing wild animals in camera-trap images with deep learning. Proc. Natl. Acad. Sci. U.S.A. **115**(25), E5716–E5725 (2018)
64. Pasternack, J., Roth, D.: Comprehensive trust metrics for information networks. In: Proceedings of the Army Science Conference (ASC), Orlando, Florida, December 2010.
65. Pasternack, J., Roth. D.: Knowing what to believe (when you already know something). In: Proceedings of International Conference on Computational Linguistics (COLING), pp. 877–885 (2010).

66. Pei, S., Kandula, S., Shaman, J.: Differential effects of intervention timing on COVID-19 spread in the United States. medRxiv preprint, posted 20 May 2020. https://doi.org/10.1101/2020.05.15.20103655. Accessed 31 May 2020
67. Pekeč, S., Venable, K.B. (eds.): ADT 2019. LNCS (LNAI), vol. 11834. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-31489-7
68. Perry, J., Gupta, D., Feigenbaum, J., Wright, R.N.: Systematizing secure computation for research and decision support. In: Abdalla, M., De Prisco, R. (eds.) Security and Cryptography for Networks (SCN 2014). LNCS, vol. 8642. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10879-7_22.
69. Pluchinotta, I., Kazakçi, A.O., Giordano, R., Tsoukiàs, A.: Design theory for generating alternatives in public decision making processes. Group Decis. Negot. **28**(2), 341–375 (2019). https://doi.org/10.1007/s10726-018-09610-5
70. Rios Insua, D., French, S. (eds.): e-Democracy. Springer, Dordrecht (2010). https://doi.org/10.1007/978-90-481-9045-4
71. Roberts, F.S.: Computer science and decision theory. Ann. Oper. Res. **163**, 209–253 (2008)
72. Roberts, F.S.: From football to oil rigs: risk assessment for combined cyber and physical attacks. J. Benefit-Cost Anal. **10**, 251–273 (2019)
73. Roberts, F.S.: Measurement of biodiversity: richness and evenness. In: Kaper, H.G., Roberts, F.S. (eds.) Mathematics of Planet Earth: Protecting Our Planet, Learning from the Past, Safeguarding for the Future, pp. 203–224. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-22044-0_8
74. Roberts, F.S.: Socially responsible facial recognition of animals (2020, in preparation)
75. Rose, A.: Economic consequence analysis of maritime cyber threats. In: DiRenzo, J.D., Drumhiller, N.K., Roberts, F.S. (eds.) Issues in Maritime Cyber Security, pp. 321–356. Westphalia Press, Washington, DC (2017)
76. Rosenzweig, C., Solecki, W.: Advancing Tools and Methods for Flexible Adaptation Pathways and Science Policy Integration. New York City Panel on Climate Change 2019 report. Annals NY Acad. Sci. 1439 (2019)
77. Rosoff, H., John, R.S., Burns, W., Siko, R.: Structuring uncertainty and conflicting objectives for life or death decisions following an urban biological catastrophe. Integr. Disaster Risk Manage. J. **2**(1), 1–21 (2012)
78. Rosoff, H., John, R.S., Prager, F.: Flu, risks, and videotape: escalation of fear and avoidance behavior. Risk Anal. **32**(4), 729–743 (2012)
79. Rossi, F., Tsoukias, A. (eds.): ADT 2009. LNCS (LNAI), vol. 5783. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04428-1
80. Schwartz, M., Machulak, M.: Securing the Perimeter: Deploying Identity and Access Management with Free Open Source Software. APress, New York (2018)
81. Sturgis, L.A. Smythe, T.C., Tucci, A.E.: Port recovery in the aftermath of hurricane Sandy: improving port resiliency in the era of climate change. Center for New American Security, Washington, DC, August 2014
82. Tebaldi, C., Strauss, B.H., Zervas, C.E.: Modelling sea level rise impacts on storm surges along US coasts. Environ. Res. Lett. **7**, 014032 (2012)
83. Tendall, D.M., et al.: Food system resilience: defining the concept. Global Food Secur. **6**, 17–23 (2015)
84. The 9/11 Commission: The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (2014). https://fas.org/irp/offdocs/911commission.pdf. Accessed 31 May 2020
85. Turner, B.L., II.: Vulnerability and resilience: coalescing or paralleling approaches for sustainability science? Global Environ. Change **20**, 570–576 (2010)
86. Valletta, J.J., Torney, C., Kings, M., Thornton, A., Jmadden, J.: Applications of machine learning in animal behavior studies. Anim. Behav. **124**, 203–220 (2017)

87. Wagstaff, J.: All at sea: Global shipping fleet exposed to hacking threat. Reuters, 23 April 2014. https://www.reuters.com/article/2014/04/23/tech-cybersecurity-shipping-idUSL3N0N402020140423. Accessed 21 Feb 2015
88. Zhao, W., Villaseca, F.E.: Byzantine fault tolerance for electric power grid monitoring and control. In: Proceedings of the 2008 International Conference on Embedded Software and Systems, pp. 129–135. IEEE Computer Society (2008)
89. Zhao, C., et al.: Secure multi-party computation: theory practice applications. Inf. Sci. **476**, 357–372 (2019). https://doi.org/10.1016/j.ins.2018.10.024