Review
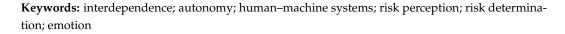
Risk Determination versus Risk Perception: A New Model of Reality for Human–Machine Autonomy

William Lawless (ID)

Department of Mathematics, Sciences and Technology, Paine College, Augusta, GA 30901, USA;
w.lawless@icloud.com

Abstract: We review the progress in developing a science of interdependence applied to the determinations and perceptions of risk for autonomous human–machine systems based on a case study of the Department of Defense's (DoD) faulty determination of risk in a drone strike in Afghanistan; the DoD's assessment was rushed, suppressing alternative risk perceptions. We begin by contrasting the lack of success found in a case study from the commercial sphere (Facebook's use of machine intelligence to find and categorize "hate speech"). Then, after the DoD case study, we draw a comparison with the Department of Energy's (DOE) mismanagement of its military nuclear wastes that created health risks to the public, DOE employees, and the environment. The DOE recovered by defending its risk determinations and challenging risk perceptions in public. We apply this process to autonomous human–machine systems. The result from this review is a major discovery about the costly suppression of risk perceptions to best determine actual risks, whether for the military, business, or politics. For autonomous systems, we conclude that the determinations of actual risks need to be limited in scope as much as feasible; and that a process of free and open debate needs to be adopted that challenges the risk perceptions arising in situations facing uncertainty as the best, and possibly the only, path forward to a solution.

Keywords: interdependence; autonomy; human–machine systems; risk perception; risk determination; emotion

1. Introduction

We review the progress in developing a science of interdependence applied to the determinations and perceptions of risk for autonomous human–machine systems based on a case study of the Department of Defense's (DoD) faulty determination of risk in a drone strike in Afghanistan; the DoD's assessment was rushed, suppressing alternative risk perceptions, possibly the result of an emotional response. We begin by contrasting the lack of success found in a case study from the commercial sphere (Facebook's use of machine intelligence to find and categorize "hate speech"). Then, after the DoD case study, we draw a comparison with the Department of Energy's (DOE) mismanagement of its military nuclear wastes that created health risks to the public, DOE employees, and the environment. The DOE recovered by defending its risk determinations and challenging risk perceptions in public. We apply this process to autonomous human–machine systems. The result from this review is a major discovery about the costly suppression of risk perceptions to best determine actual risks, whether for the military, business, or politics. For autonomous systems, we conclude that the determinations of actual risks need to be limited in scope as much as feasible; and that a process of free and open debate needs to be adopted that challenges the risk perceptions arising in situations facing uncertainty as the best, and possibly the only, path forward to a solution. In our conclusion, however, we briefly discuss that emotion must not be allowed to be a driver of a decision in a rush to judgment.

1.1. Situation

The number of robots and drones in use around the world is increasing dramatically. In 2019, there were about 373,000 industrial robots sold, with a prevalence ranging from about 1 per twenty workers in Singapore to about 2 per hundred workers in the USA (www.statista.com/topics/1476/industrial-robots, accessed on 20 December 2021). The World Robotics 2020 summary of Industrial Robots report found a total of 2.7 million robots already working across the world, or about 3 robots for every 10,000 humans.

In the USA (www.faa.gov/uas/resources/by-the-numbers, accessed on 20 December 2021), there are about 866,000 drones, with about 40 percent registered for commercial use; the number estimated in 2021 was approaching almost 2 million (seedscientific.com/drone-statistics/, accessed on 20 December 2021). In 2019, almost 100 countries had military drones [1]. Overall, however, none of the drones and robots presently in use are autonomous.

To operate the robots, drones, self-driving vehicles, and other machines in various states of autonomy, artificial intelligence (AI) and machine learning (ML) are necessary. Machine learning, in particular, has already made extraordinary strides in science, medicine, military matters, and society in general, and more "profound changes are coming" [2].

Before we begin, we provide a Table of the Acronyms (Table 1) to be found in this paper by providing a reference to help readers.

Table 1. A list of acronyms.

Artificial Intelligence	AI
Machine Learning	ML
U.S. Department of Defense	DoD
U.S. Department of Energy	DOE
Islamic State Khorasan	ISIS-K
Associated Press	AP
DOE Citizens Advisory Board	CAB
Engineering risk perspective	ERP
Perceived risks perspective	PRP
Hamid Karzai International Airport, Kabul, Afghanistan	HKIA
Lethal Autonomous Weapon Systems	LAWS
Self-driving autonomous vehicle	AV
Central Intelligence Agency	CIA
Structural Entropy Production	SEP
Maximum Entropy Production	MEP
U.S. DoD's Central Command	CENTCOM
U.K.'s Foreign, Commonwealth and Development Office	FCDO
China's Communist Party	CCP
DoD's Commercial Off-the-Shelf	COTS

1.2. Case Studies

1.2.1. A Commercial Case Study

Categorizing actual risks with AI's machine intelligence is a difficult problem. It is the reason why the self-driving cars that come to rely on machine learning operate repeatedly over closed courses. From Mantica [3], "Self-driving cars are powered by machine learning algorithms that require vast amounts of driving data in order to function safely". As reported in the Wall Street Journal [4], even Facebook, probably the operator of one of the

most sophisticated machine learning algorithms, has had limited success detecting "hate speech" with its system of learning machines. In this article, Facebook's classifiers have labeled the video of a car wash as a first-person shooter event, and the video of a shooting as a car crash. Queried for this article, Sheryl Sandberg, Facebook's Chief Operating Officer, responded that Facebook's algorithms detected 91 percent of the 1.5 million posts it had detained for violating its hate policies. Casting doubt on Sandberg's claim, however, the software engineers and scientists at Facebook had earlier reported to BuzzFeed [5] that,

> Using internal Facebook data and projections to support their points, the data scientist said in their post that roughly 1 of every 1000 pieces of content—or 5 million of the 5 billion pieces of content posted to the social network daily— violates the company's rules on hate speech. More stunning, they estimated using the company's own figures that, even with artificial intelligence and third-party moderators, the company was "deleting less than 5 [percent] of all of the hate speech posted to Facebook. . . We might just be the very best in the world at it", he wrote, "but the best in the world isn't good enough to find a fraction of it".

One of the conclusions to be drawn about machine learning (ML), including its use at Facebook, one of its most sophisticated users, is that ML is context dependent [6]. Thus, ML is unlikely to be able to provide solutions to problems when a human–machine team is faced by uncertainty or conflict. To produce autonomy, we must look elsewhere.

1.2.2. A Military Case Study

A categorization problem similar to Facebook's exists in determining the risk posed by potential adversaries in combat theaters. For example, the last U.S. missile thought to have been fired by a U.S. drone in Afghanistan occurred after a lengthy surveillance of a car on 29 August 2021, leading the U.S. military to conclude that the car contained a bomb that posed the risk of an imminent threat to U.S. troops at Kabul's airport. In remarks by the U.S. President, he said that:

> We will maintain the fight against terrorism in Afghanistan and other countries. We just don't need to fight a ground war to do it. We have what's called over-the-horizon capabilities, which means we can strike terrorists and targets without American boots on the ground—or very few, if needed. We've shown that capacity just in the last week. We struck ISIS-K remotely, days after they murdered 13 of our service members and dozens of innocent Afghans.

That was the planned result sought by the DoD's risk assessment for this particular car. However, an investigation by the New York Times [7] began to raise doubts about the interpretation and justification of the drone attack, doubts about whether explosives were in the vehicle, doubts about whether the driver was a terrorist, and doubts about whether the missile's explosion generated secondary explosions. When the DoD was confronted by a follow up story seven days later, the New York Times began to suspect that the U.S. military was becoming defensive [8]:

> Defense Secretary Lloyd J. Austin III and Gen. Mark A. Milley, the chairman of the Joint Chiefs of Staff, have said that the missile was launched because the military had intelligence suggesting a credible, imminent threat to Hamid Karzai International Airport in Kabul, where U.S. and allied troops were frantically trying to evacuate people. General Milley later called the strike "righteous".

Subsequent news accounts (e.g., [9]), however, indicated that the attack was a mistake that may have killed 10 civilians, of which seven were children. To investigate formally, U.S. Air Force Lt. Gen. Sami D. Said, Inspector General of the Air Force, began to conduct a formal investigation of the drone attack:

> The service is asking Said to consider whether anyone in the chain of command should be held accountable for what Marine Gen. Frank McKenzie, the head of U.S. Central Command, called a tragic mistake.

In addition to the formal U.S. Air Force investigation by Lt. Gen. Said, the Department of Defense's (DoD) inspector general also launched an investigation into the U.S. drone strike in Kabul, DoD officials announced [10]. Moreover from the AP, an apology had already been issued by the U.S. military, senior Pentagon officials, and personally by the U.S. Defense Secretary [11] for the August 29 drone strike in Kabul, calling it a "tragic mistake". Furthermore [12],

> A senior U.S. Democrat said on Thursday that multiple congressional committees will investigate a drone strike that killed 10 Afghan civilians last month, to determine what went wrong and answer questions about future counter-terrorism strategy.

The extraordinary financial costs and loss of prestige from this erroneous risk assessment had also made news. From Reuters news service [13],

> The Pentagon has offered... payments to the family of 10 civilians who were killed in a botched U.S. drone attack in Afghanistan in August during the final days before American troops withdrew from the country. The U.S. Defense Department said it made a commitment that included offering "ex-gratia condolence payments"... [and] relocation to the United States. Colin Kahl, the U.S. Under Secretary of Defense for Policy, held a virtual meeting on Thursday with Steven Kwon, the founder and president of Nutrition [and] Education International, the aid organization that employed Zemari Ahmadi, who was killed in the 29 August 2021 drone attack... Ahmadi and others who were killed in the strike were innocent victims who bore no blame and were not affiliated with Islamic State Khorasan (ISIS-K) or threats to U.S. forces...

The example of the tragic drone strike in Afghanistan given in this section and the quote above will be discussed further in Section 1.3.3.

1.2.3. A Case Study of Department of Energy's (DOE) Military Nuclear Wastes

Until 1985, DOE nuclear waste operations had caused extraordinary damage across the U.S. from the mismanagement of its military nuclear wastes. The cleanup was estimated at up to USD 200 billion for its two largest sites, the Hanford facility in Washington State and the Savannah River Site (SRS) in South Carolina [14]. From [15], the perceptions, right or wrong, created by the DOE's mishandling of its military nuclear wastes was to create a "profound state of distrust that cannot be erased quickly or easily" (p. 1603). To begin to recover trust, to guide its risk determinations, and to better assess the public's risk perceptions, the DOE installed nine public committees to advise the DOE; these committees made decisions by either seeking consensus (e.g., at Hanford) or by majority rules (e.g., SRS). The results formed a natural experiment. By rapidly accelerating the cleanup of the DOE's mismanagement at SRS compared to its slow-down at Hanford, we found that majority-rule decisions by DOE's Citizen Advisory Boards (CAB) were superior to those made by consensus-seeking CAB decisions [14,16].

Regarding consensus-seeking elsewhere, a White Paper reporting on a study of improving decision making for Europe concluded, "The requirement for consensus in the European Council often holds policy-making hostage to national interests in areas which Council could and should decide by a qualified majority" ([17], p. 29). The problem with majority rule is that it does not protect minority interests; conversely, the problem with consensus-seeking is that it provides a minority, say an authoritarian leader, the power to block any action desired, becoming minority control [14].

Minority control is sought even in China, which recently concluded a major plenum of the Chinese Communist Party, producing a formal resolution on party history that officially elevates General Secretary Xi Jinping to the highest political position within the Chinese Communist pantheon [18]:

> With this resolution the party has elevated Mr. Xi and "Xi Jinping Thought" to a status that puts them beyond critique. As both are now entrenched as objective

historical truth, to criticize Mr. Xi is to attack the party and even China itself. Mr. Xi has rendered himself politically untouchable.

Minority control is best exemplified by command economies where all economic activity is controlled by a central authority. From the editors of the Britannica [19],

Command economies were characteristic of the Soviet Union and the communist countries of the Eastern bloc, and their inefficiencies were among the factors that contributed to the fall of communism in those regions in 1990–91.

1.3. How to Fix Faulty Risk Assessments?

A fix to the faulty risk assessment for the use human–machine drone teams begins by decomposing risk assessment into two parts: an engineering risk determination or assessment (cost-benefit analysis), and the perceived risks.

1.3.1. Engineering Risk Perspective (ERP)

From an engineering risk perspective (ERP), can the risks to operate a machine or human–machine system as requested be assessed? Can the system become autonomous? Can the machine solve the problem it faces? How much uncertainty exists in the problem faced by the machine system? For a system as complicated as the one implicated in the drone attack, are handoffs between teams of humans and machines a part of the problem? (www.ready.gov/risk-assessment, accessed on 20 December 2021).

1.3.2. Perceived Risks Perspective (PRP)

Risk perspectives are subjective estimates of a hazard constructed by intuition, emotion, and the media; these risk assessments are followed by risk communications in the attempt to persuade the public about the actual risks derived from an engineering perspective [20]. Perceived risk in nuclear matters has been strongly linked to trust [15]. From [21], risk perceptions arise from "actual threats, sights, sounds, smells, and even words or memories associated with fear or danger", promoting an anxiety about risks, however, that may be sufficient to create "risks all by itself" (p. 3).

1.3.3. Discussion: Mismanagement, the Loss of Trust, and Its Recovery

Returning to the military case study, like the DOE's recovery of trust after its mismanagement, a critical step in fixing a mismanagement problem that leads to the loss of trust is an open assessment such as the DOE's of the causes of its own mismanagement of military nuclear wastes. To its credit, the DoD [22] openly briefed the press about its investigation, while its report remains classified because, according to Lt. Gen. Said, its author, "the sources and methods and tactics, techniques and procedures used in executing such strikes are classified". For the report, Said interviewed "29 individuals, 22 directly involved with this strike, and under oath".

Said [22] described the context at the moment before the strike was launched as a process that "transpired over eight hours". He stated that "the risk to force at HKIA and the multiple threat streams that they were receiving of an imminent attack, mindful that, three days prior, such an attack took place, where we lost 13 soldiers–or lost 13 members and a lot of Afghan civilians". Moreover, continued Said, the U.S. military was one day away from leaving Afghanistan [22], (https://military-history.fandom.com/wiki/Hamid_Karzai_International_Airport, accessed on 21 March 2022).

. . . so the ability for defense had declined. We're concentrated in one location, with a lot of threat streams indicating imminent attacks that looked similar to the attack that happened three days prior. So you can imagine the stress on the force is high and the risk to force is high, and not appreciating what I'm about to say through that lens I think would be inappropriate.

Said [22] added that the strike "was unique in the sense that it was a self defense strike . . . the norm . . . [is] where you have a long time to do things like pattern of life. You

have days to assess the intelligence and determine how you're going to execute the strike. It's a very different construct and very different execution".

In his report [22], Said "confirmed that the strike resulted in the death of 10 Afghan civilians, including three men and seven children. [However, the US Military] Individuals involved in this strike, interviewed during his investigation, truly believed at the time that they were targeting an imminent threat to U.S. forces on HKIA. The intended target of the strike, the vehicle, the white Corolla, its contents and occupant were genuinely assessed at the time to be a threat to U.S. forces". Said attributed the DoD's erroneous risk determination to an "aggregate process breakdown" involving many people.

Per Said, the DoD's [22] risk determination became a one-sided (biased) risk perception. He stated that the

> assessment was primarily driven by interpretation of intelligence and correlating that to observe movement throughout an eight hour window in which the vehicle was tracked throughout the day before it was ultimately struck. Regrettably, the interpretation or the correlation of the intelligence to what was being perceived at the time, in real time, was inaccurate. In fact, the vehicle, its occupant and contents did not pose any risk to U.S. forces . . . The investigation found no violation of law, including the law of war. It did find execution errors . . . combined with confirmation bias and communication breakdowns that regrettably led to civilian casualties.

As part of his investigation, Said made three recommendations: First, adopt procedures in a strike cell in a similar situation where the military is time-constrained to act quickly to exercise self-defense in urban terrain and to interpret or correlate intelligence rapidly, with procedures that mitigate the risk of a confirmation bias. Second, enhance situational awareness by sharing information thoroughly within the confines of the strike cell and outside the cell to those supporting elements located elsewhere. Third, include an assessment in the cell of the presence of civilians, specifically children, or anything that may magnify the costs of an erroneous decision, that is, the "severity" of a misjudgment.

However, in addition, Said [22] recommended a process of "red-teaming"; whatever the risk determination, an independent team should be assigned to push back against the one-sided interpretation to break "confirmation bias." This conclusion is similar to the DOE's. To help the DOE recover its lost prestige and to regain the public's trust, we drew conclusions similar to the DoD's Lt. Gen. Said's fourth recommendation that the confrontation among competing perceptions that are decided among citizen advisors by majority rule accelerated the DOE's cleanup at its Savannah River Site compared to the consensus-seeking rules used at its Hanford site [14,16].

2. A Work-in-Progress: Future Autonomous Systems

Autonomous Systems

The importance of a process that checks risk determinations to uncover errors becomes even more important when autonomous systems are introduced to the battlefield. For these, legal limits are being considered. From the Congressional Research Service [23],

> Lethal Autonomous Weapon Systems (LAWS) are a class of weapon systems capable of independently identifying a target and employing an onboard weapon system to engage and destroy the target without manual human control. LAWS require computer algorithms and sensor suites to classify an object as hostile, make an engagement decision, and guide a weapon to the target. This capability would enable the system to operate in communications-degraded or -denied environments where traditional systems may not be able to operate. LAWS are not yet in widespread development, and some senior military and defense leaders have expressed concerns about the ethics of ever fielding such systems. For example, in 2017 testimony before the Senate Armed Services Committee, then-Vice Chairman of the Joint Chiefs of Staff General Paul Selva stated, "I do

not think it is reasonable for us to put robots in charge of whether or not we take a human life".

Presently, there are no laws prohibiting the development of LAWS, but national and international groups have begun to discuss the issue and to propose rules. Thirty countries or more have called for a ban on these systems due to ethical and moral considerations. Formal regulation or guidelines for development and use are being proposed. The DoD has established military guidelines for the development and fielding of LAWS to ensure that the law is followed including the law of war, including treaties, rules for weapon system safety, and the DoD's rules of engagement [23].

Mayes [24] compared LAWS systems with self-driving autonomous vehicles (AVs). In this comparison, Mayes concluded that AVs today are robots that can exhibit the same skills as humans when navigating, parking, turning, backing up, etc., but these robot AVs must still be overseen by humans today:

> Most new cars sold today are Level 1 with features such as automated cruise control and park assist. A number of companies including Tesla, Uber, Waymo, Audi, Volvo, Mercedes-Benz, and Cadillac have introduced Level 2 vehicles with automated acceleration and braking and are required to have a safety driver in the front seat available to take over if something goes wrong . . . Waymo has a fleet of hybrid cars in Phoenix, Arizona, that it is using to test and develop Level 5 technology specifically to pick up and drop off passengers (for a review of the levels of autonomy in vehicles, see https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety, accessed on 20 December 2021).

To delve more deeply into the risks arising with autonomy, we briefly review a mathematical physics model. Afterwards, we review the predictions and implications of the model. While the model is simple, its implications are not.

First, we assume that a major part of modeling is to simplify a chosen model to the extent possible, as long as it can recreate the event observed. However, the simplest group of models, game theory and agent-based models, assume closed systems, and are unable to capture the social events observed (e.g., [25,26]).

Second, needed instead are open-system models, the most challenging type of model, to address situations such as the failed drone strike in Afghanistan. However, for open-systems, their chief characteristic is uncertainty; e.g., in economics, Rudd [27] cites the essence of his discipline's inability to recreate the effects of inflation when faced by uncertainty; in the controversial first sentence of his new paper, he describes this failure:

> Mainstream economics is replete with ideas that "everyone knows" to be true, but that are actually arrant nonsense.

3. Mathematical Model

Applied to intelligent systems, the chief characteristic in response to uncertainty is an interdependent reactivity to the perceived risks that may arise and may or may not be suppressed. For an open-system model of teams, we propose that a trade-off exists between uncertainty in the entropy produced by the structure of an autonomous human–machine system, $\Delta Structure$, and uncertainty in the entropy produced by a team's performance, $\Delta Performance$, with c as a constant, for the two factors of structure entropy production (SEP) and performance entropy production (MEP) (for details, see [28]), giving:

$$\Delta(structure) * \Delta(performance) \approx c \approx \Delta(\text{SEP}) * \Delta(\text{MEP}) \tag{1}$$

We read Equation (1) as follows: The uncertainty in the Structural Entropy Production times uncertainty in the Maximum Entropy Production by a team's performance is a constant (unknown presently). For the rest of this article, we review the predictions from Equation (1), which are counter-intuitive. To assist the reader, we have added a Table of Predictions and Findings in Table 2.

Table 2. Predictions and Findings.

Section	Factors	Prediction
Section 3.1	Structure of an autonomous team: Good fit	Decreased SEP makes increased MEP more likely, if focused
Section 3.1.1	Structure of an autonomous team: Bad fit	Increased SEP, reduced MEP
Section 3.1.2	Mergers, alliances, defense treaties	Seeking fitness, increased competitiveness, less vulnerability
Section 3.2	Concepts and behavior	The more accurate a concept, the less valid it likely becomes
Section 3.2.1	Perceptions and interpretations	A wide spectrum of beliefs
Section 3.3	Rational decisions	Knowledge (K) signified by zero entropy production
Section 3.4	Deception	Elusive as SEP is minimized
Section 3.5	Innovation	Increases across a region where MEP is maximized
Section 3.6	Minority control or Coercion	Produces low SEP and low MEP
Section 3.7	Solutions to uncertainty	Challenges that test ideas; e.g., "Red teams"; checks and balances

3.1. Structure and Performance

Equation (1) indicates that, as the structure of an autonomous team is reduced to a minimum (as SEP goes to zero), the performance of a good team is more likely to increase to a maximum (MEP is likely to increase to a maximum if the team can focus the available free energy to achieve its mission; this outcome is somewhat like focusing a telescope to be able to produce a better image when the telescope is also pointed in the right direction).

3.1.1. Structure and Performance Bad Team

In contrast to a good team, when a team is unable to find the best fit among its team members, its SEP increases, it wastes the free energy available to it, and it is unable to reach MEP for the performance of its mission.

3.1.2. Mergers

Experience helps humans to sort through misperceived risk perceptions. In business, the motivation to reduce uncertainty and the fittedness that results with business mergers combine to offer examples of the risks in play in open systems. Reducing the risk from uncertainty is the driving motivation for mergers in the market place; e.g., the eBay–PayPal deal is a general example [29]; a more relevant example of a merger for this paper is FiscalNote's acquisition of Forge.AI, Inc. to obtain the technology to help it better model risk for autonomous vehicles [30]. For driverless cars, however, Aurora Innovation acquired Uber's self-driving cars last year in the hope that the risks determined to exist for self-driving vehicles had been reduced, but concluding subsequently that the "technology isn't there yet" [31]. The failure to achieve or maintain fittedness increases the risk of breakups or spin-offs, such as has happened with General Electric, an industrial giant in the late 20th century renowned for its management prowess (led by Jack Welch from 1981–2001, considered by many as the greatest leader of his time [32]; Welch was succeeded by Jeff Immelt, a leader who was slow to see the emerging financial risks [33]), but in recent years, GE faced increasing risks as it has struggled to survive (e.g., [34]).

In conclusion, based on Equation (1), the construction of a team from our brief discussion of mergers is governed not by logic, but by a trial and error process. Once the right fit is obtained, it is characterized by least SEP from adding or replacing a team member that reduces the structural entropy produced.

3.2. Concepts and Behavior

Applying Equation (1) to concepts and action results in a tradeoff: as uncertainty in a concept reaches a minimum, the overriding goal of social scientists, uncertainty in the behavioral actions covered by that concept increases exponentially, rendering the

concept invalid, the result that has been found for numerous concepts, e.g., self-esteem [35], implicit attitudes [36], or ego-depletion [37]. These problems with concepts have lead to the widespread demand for replication [38]. However, the demand for replication more or less overlooks the larger problem with the lack of generalizability arising with what amounts to the use of strictly independent data [39].

3.2.1. Perceptions and Interpretations

Applying Equation (1) to risk determination and then risk perception, if a risk determination indicates that an autonomous structure (of, say, a team) is perfect, its structure should generate no information in the limit, i.e., zero SEP [28]. Such a situation would provide an opportunity for an autonomous team to generate MEP to achieve or perform its mission. Regarding risk perception, however, human witnesses to events can generate an infinite spectrum of possible interpretations, including nonsensical and even dangerous ones as experienced by the DoD's unchallenged decision to launch what became an erroneous drone attack. In this regard, social science appears to be more interested in "changing the ingrained attitudes" associated with suppression ([40], p. 376), rendering itself of little help regarding uncertain contexts, amplified in an Editorial by the new editor of the *Journal of Personality and Social Psychology: Interpersonal Relations and Group Processes* who seeks to publish articles to reflect that "our field is becoming a nexus for social-behavioral science on individuals in context" [41]. Our problem with the editor's description of context is that it assumes certainty for a given context.

The result is an over-focus on individual biases and not on generalization beyond a concept's target application. Focusing too much on cognitive biases is a form of self-inflicted blindness that overlooks the greater value of applying Equation (1) jointly to cognition and behavior to gain a larger, more valuable, scientific picture.

3.3. Rationality

There are multiple ways to look at rationality. Mann [42] conceived of a rational approach to the structure of teams, but his project failed when uncertainty in the environment occurred, especially when confronted by competition or conflict. Alternatively, the mathematics of quantum mechanics is considered to be rational, but an interpretation of what it means is elusive and thus not rational [43]. We proceed with the next section in the hopes of finding a result similar to quantum mechanics, even if the interpretation of autonomous systems remains out of reach, as it has with intuitions about quantum mechanics.

Martinez and Sequoiah-Grayson [44] see the relation between logic and information as bi-directional, creating a tradeoff as in Equation (1). Information for rational decisions leads to an inference that underlies the intuitive understanding of standard logical notions (e.g., the process that makes implicit information explicit) and computation. Conversely, logic is the formal framework to study information to achieve logical decisions. Martinez and Sequoiah-Grayson specify that,

> Acquiring new information corresponds to a reduction of that range, thus reducing uncertainty about the actual configuration of affairs ... an epistemic action is any action that facilitates the flow of information ... The Information-as-correlation stance focuses on information flow as it is licensed within structured systems formed by systematically correlated components ... the correlations between the parts naturally allow for 'information flow' ... Formally speaking, negative information is simply the extension-via-negation of the positive fragment of any logic built around information-states ...

What Martinez and Sequoiah-Grayson leave out, however, is that bistable information collected from an orthogonal pair of teammates does not correlate (e.g., a husband–wife; a cook–waiter; a mechanic–pilot), motivating the need to test the information collected, especially the determinations of risk so eloquently raised by Lt. Gen. Said's report [22], by Lawless and colleagues [16], and by Justice Ginsburg [45]. From Pinker [46], goals need not be rational, however,

> ... rationality emerges from a community of reasoners who spot each other's fallacies ... [Rational thinking] is the ability to use knowledge to obtain goals. But we must use reason to choose among them when they conflict.

Risk assessments and risk perceptions form a core part of rational decision-making. Thagard [47] has studied whether science is rational, concluding, "A person or group is rational to the extent that its practices enable it to accomplish its legitimate goals". Applied to science, "scientific theories should make predictions about observable phenomena [that] aims for explanation as well as truth ...".

For Wilson [48], the unity of knowledge must be achieved through the scientific method. Wilson's goal is to reduce subjective determinations. As an evolutionary scientist, Wilson writes that we should "have the common goal of turning as much philosophy as possible into science". Respectfully, we disagree; Wilson does not perceive the value of society's contribution to its own evolution with its evolution of technology as both co-evolving [49].

Further contradicting Martinez and Sequoiah-Grayson, machine learning, like Shannon's [50] information theory, is restricted to i.i.d. data (independent, identically distributed data; in [39]). However, and despite great effort [42], rationality is limited to non-conflictual and clearly certain contexts. Machine learning is context dependent [6].

Similarly, game theory and agent-based models are rational models based on closed systems. Games work well when the context is pre-set, when a situation can be clearly established, or when the payoffs are well-known, but the evidence suggests that game theory may not work when facing uncertainty, a flaw of rational models [42]. As an example from the fleet, the use of war games results in "preordained proofs", per retired General Zinni [51]; that is, users (e.g., engineers) choose a game for a given context to obtain a desired outcome.

3.4. Deception

Part of the difficulty of the problem with calculating a risk assessment of a terrorist strike is that terrorists often cloak their activities in deception. Deception's use in cloak and dagger work with human intelligence is needed and is well described by Luttwak [52]:

> CIA or other field officers who speak local languages well enough to pass, can physically blend in, identify insurgents, uncover their gatherings and direct attacks on them.

The use of deception occurs in businesses, too. From the Wall Street Journal, Amazon has been charged with using deception against its marketers by stealing the designs of the companies it markets [53]:

> Amazon.com Inc. AMZN 3.31% employees have used data about independent sellers on the company's platform to develop competing products, a practice at odds with the company's stated policies.

If true, deception occurs to those successful businesses that use Amazon to market their goods. The charge against Amazon is currently being investigated by Congress [54]. Amazon counters in its privacy policy that: "We know that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly".

Based on Equation (1), however, if deception is used to minimize the presence of an adversary inside of an opponent's team, it succeeds by minimizing the team's SEP within which the deceiver has been inserted. Deception is difficult to uncover. To uncover deception requires a challenge to the appearance of a normal, smooth, or well-running operation, as may often occur with cyber-security [55]. For example, from the Wall Street Journal [56],

> Undercover Taliban agents—often clean-shaven, dressed in jeans and sporting sunglasses—spent years infiltrating Afghan government ministries, universities,

businesses and aid organizations. Then, as U.S. forces were completing their withdrawal in August, these operatives stepped out of the shadows in Kabul and other big cities across Afghanistan, surprising their neighbors and colleagues. Pulling their weapons from hiding, they helped the Taliban rapidly seize control from the inside. The pivotal role played by these clandestine cells is becoming apparent only now, three months after the U.S. pullout. At the time, Afghan cities fell one after another like dominoes with little resistance from the American-backed government's troops. Kabul collapsed in a matter of hours, with hardly a shot fired. "We had agents in every organization and department," boasted Mawlawi Mohammad Salim Saad, a senior Taliban leader who directed suicide-bombing operations and assassinations inside the Afghan capital before its fall. "The units we had already present in Kabul took control of the strategic locations".

Deception can turn inward, too, in the form of self-deception. If a team is not considering the effect a particular member has on the entropy produced by its own team's structure, consequently, the team will become more vulnerable, a form of denial by the members chosen or the processes adopted, signified by an increase in SEP or a reduction in MEP and more likely both (e.g., in the Russian invasion of Ukraine, many of the Russian troops may have feared alerting their leaders to an inferior outcome that may have cast them in a bad light).

As an example of self-deception, in his book, Robison [57], an award winning investigative journalist for Bloomberg and Bloomberg Businessweek, wrote about the management and engineering dysfunction that led to tragic accidents within Boeing aircraft. Boeing is an industrial titan in aviation, from the beginning of commercial flight, bombers in World War II, and landings on the moon. Boeing has been an anchor in the U.S. economy; however, in 2018 and 2019, the two crashes of the Boeing 737 MAX killed 346 people, exposing a scandal of corporate malfeasance, the biggest crisis in Boeing's history. Robison reveals how Boeing's broken culture in its race to beat Europe's Airbus and reward its executives led it to skimp on testing, pressure its employees, and deceive its regulators and itself to certify planes into service by ignoring safety or properly preparing pilots for flight.

Using deception in a given context may poison the data that machine learning needs to learn. From Galle [58], The Achilles' heel of machine learning is the machine's ability to learn from examples. By using deception to poison these example datasets, adversaries can corrupt the machine's training process, potentially causing the United States to field unreliable or dangerous assets.

What effect is AI having on deception? In his new book, Zegart [59] writes that,

> Artificial intelligence is creating deepfake video, audio, and photographs so real, their inauthenticity may be impossible to detect. No set of threats has changed so fast and demanded so much from intelligence.

Finally, deception can take a even darker turn. In an essay in the New York Times Magazine [60],

> Pegasus was "zero click"—unlike more common hacking software, it did not require users to click on a malicious attachment or link—so the Americans monitoring the phones could see no evidence of an ongoing breach. They couldn't see the Pegasus computers connecting to a network of servers around the world, hacking the phone, then connecting back to the equipment at the New Jersey facility. What they could see, minutes later, was every piece of data stored on the phone as it unspooled onto the large monitors of the Pegasus computers: every email, every photo, every text thread, every personal contact. They could also see the phone's location and even take control of its camera and microphone. F.B.I. agents using Pegasus could, in theory, almost instantly transform phones around the world into powerful surveillance tools—everywhere except in the United States.

Phantom [60] allows American law enforcement and spy agencies to gain intelligence by extracting and monitoring critical data from mobile devices. It is a solution independent of a service provider, and that requires no cooperation from AT&T, Verizon, Apple, or Google. This system is able to "turn your target's smartphone into an intelligence gold mine".

3.5. Innovation: A Tradeoff between Innovation and Suppression

Misperceptions can cause problems. In contrast, competing risk misperception is one of the motivating drivers of innovation. It requires an interdependence between society and technology that allows both to co-evolve [49]. Exemplified by an op-ed in the Wall Street Journal, innovation more likely occurs in small businesses, increasing risks to large businesses which seek to mitigate their perceived risks by asking Congress to adopt regulations that protect their interests [61]:

> Research in recent years has demonstrated that new businesses account dispro-portionately for the innovations that drive productivity growth, economic growth and new job creation ... The Platform Competition and Opportunity Act ... would restrict and in some cases ban the acquisition of startups by larger compa-nies. Ostensibly, the goal is to foster competition by preventing dominant online platforms from expanding their sway through acquisitions.

However, this proposed legislation risks hurting the startups it aims to benefit; observe that it is actively supported by big business [62]:

> The call for government action is part of a shifting ethos in Silicon Valley. In the past, the region has championed libertarian ideals and favored government's staying out of the way of its innovations. However, tech leaders have begun to encourage Washington to become more involved in the tech industry as competi-tion with China escalates, cyberattacks intensify and lawmakers express concerns about misinformation and censorship on social-media platforms.

Similarly, China approaches the same problem as Amazon and big business by also suppressing outright its society's "undesired" perceptions and beliefs, but in the process suppressing the animal spirits associated with emotion (from Keynes [63], pp. 161–162). The danger occurs when government steps in to "countervail the excesses that occur because of our animal spirits" (from the Akerlof and Shiller, [64], p. 9). As Keynes and others have noted, animal spirits are associated with confidence, trust, and creativity in a market; suppressing animal spirits can impede innovation (in China, see [65]).

The U.S. military has shown a similar tendency when little public attention has been paid to one of the DoD's mistakes. From the New York Times [66], near the end of the fight in Syria against Islamic State, with women and children of the once-fierce caliphate cornered in a field near a town called Baghuz, a U.S. military drone hunting for military targets saw instead the women and children by a river bank. Subsequently, American F-15E attack jets dropped bombs on them, leaving no survivors. Continuing [66],

> The Defense Department's independent inspector general began an inquiry, but the report containing its findings was stalled and stripped of any mention of the strike. "Leadership just seemed so set on burying this ...", said Gene Tate, an evaluator who worked on the case for the inspector general's office and agreed to discuss the aspects that were not classified. "It makes you lose faith in the system when people are trying to do what's right but no one in positions of leadership wants to hear it". Mr. Tate ... said he criticized the lack of action and was eventually forced out of his job.

However, as a result of media reports [67],

> Earlier this week, Defense Secretary Lloyd Austin ordered an investigation into a March 2019 drone strike, reported by the New York Times last month, that also allegedly killed civilians. The strike occurred on March 18 of that year, and it

killed 80 people, some of whom were civilians. CENTCOM acknowledged at the time that 80 people were killed in the strike, 16 of whom were fighters and four civilians, while the status of the other 60 people were unclear.

The media provided more details [68],

A single top secret American strike cell launched tens of thousands of bombs and missiles against the Islamic State in Syria, but in the process of hammering a vicious enemy, the shadowy force sidestepped safeguards and repeatedly killed civilians, according to multiple . . . intelligence officials.

Unlike the "red teams" recommended by Lt. Gen. Said, for this incident, a report was written to describe "the shortcomings of the process . . . [and that] the assessment teams at times lacked training and some did not have security clearances to even view the evidence" [66]. The Times reported that the assessments of the failed strike were flawed because they were performed by the same units involved in the strikes and were grading their own performance. The U.S. has since admitted the Syria strike in question was a mistake [67].

3.6. Minority Control: Coercion

There is another way to achieve low SEP. Returning to Equation (1), coercion can be used to force a team's structure to emit low levels of entropy.

Minority control with coercion is a way that humans make decisions. The weakness of minority control is that it increases uncertainty in followers; e.g., the management style of Xi Jinping, China's leader, has been evolving [69],

as the Chinese president consolidates control of the world's second-largest economy. He is widely considered the most powerful Chinese leader in a generation. He is also a micromanager who intervenes often, unpredictably and sometimes vaguely in policy matters big and small. People inside the government say that sows confusion among bureaucrats, stifles policy debate and sometimes leads to policies that aren't carefully thought-out. Some bureaucrats, unsure how far to push Mr. Xi's priorities, err on the side of aggressive interpretation, and this sometimes means reversing policies later.

Internationally, open coercion may serve to prevent conflict [70] as it has in the past when the U.S. threatened military intervention against Haiti's military coup in 1994, leading to a peaceful transfer of power back to the previously deposed president, Jean-Bertrand Aristide; but similar and open threats to intervene militarily in 1998 against Iraq's rejection of UN inspections failed to achieve a peaceful result.

In general, minority control is one way that humans make decisions (e.g., for authoritarian Cuba, see [71]; for gangs, see [72]; for consensus-seeking, see [17]). As a major new finding with Equation (1), instead of seeking the best fit to minimize structural entropy production so that an autonomous team or system can maximize entropy production (MEP) for its mission or for innovation, minority control expends the free energy available to forcibly achieve stability but also by significantly reducing MEP, the opposite of exploiting interdependence, and, working backwards, a way for a system to de-evolve (e.g., spin-offs, such as J&J, in [73]; human trafficking in Cuba; or famine in N. Korea). Further, de-evolution has a cost that requires authoritarian governments to steal technology to remain competitive; e.g., "China used cyber espionage and an insider source to get a hold of the F-35, F-22, and C-130 blueprints in 2016" [74] and drone technology [75]:

In 2018, a Chinese state-controlled company bought an Italian manufacturer of military drones. Soon after, it began transferring the company's know-how and technology . . . The takeover fits a pattern, analysts say, of Chinese state firms using ostensibly private shell companies as fronts to snap up firms with specific technologies that they then shift to new facilities in China . . . Analysts say Beijing is using such purchases to target specific needs, such as semiconductors . . . [or] night-vision sensor or . . . data-link technology . . .

But China continues apace heedless of the evidence of its failures. From the Wall Street Journal [76], Xi Jinping, China's President, has overseen a new resolution to warn the Chinese Communist party about constitutionalism and the separation of powers that China remains "on guard against the erosive influence of Western trends of political thought" to deliver China a future "that is much better than what 'Western democracies' have to offer":

China's Communist Party has issued a rare new accounting of its history that seals Xi Jinping's place in the pantheon of the country's greatest leaders . . . It sets up Mr. Xi to wield lasting influence over the country's future as he seeks a precedent-breaking third term next year . . . As leader, Mr. Xi has invoked Maoist rhetoric and tried to tamp criticism of Mao's dictatorial ways, portraying his years in power as a vital and inseparable part of China's success story . . .

China's retreat from free market and democratic government as it turns to strong-armed authoritarianism of its leader reflected by the minority control of its Communist Party (CCP) is creating severe problems. This retreat by China should cause a dramatic reduction in innovation, a conclusion supported by a recent essay by [77] who found that,

China is experiencing a slow-motion economic crisis that could undermine stability in the current regime and have serious negative consequences for the global economy . . . In December real-estate developers China Evergrande and Kaisa joined several other overleveraged firms in bankruptcy, exposing hundreds of billions in yuan- and dollar-denominated debt to default . . . Sales and prices have tumbled this year, and overleveraged builders and creditors are suffering the consequences . . . In his zeal to reassert the dominance of the Chinese Communist Party, Mr. Xi has engineered a crackdown on some of China's most innovative industries and the entrepreneurs building them . . . Mr. Xi is privileging the less productive and less innovative components of the Chinese economy while enhancing control, limiting financing and punishing entrepreneurial leaders in many leading industries . . . China's commercial aviation industry doesn't have an internationally certified jet to compete with Boeing and Airbus, despite three decades of concentrated efforts. Its biopharmaceutical industry failed to produce an effective vaccine for Covid. Steel, batteries and high-speed rail—where China is competitive—are at risk of trade retaliation due to environmentally harmful production practices and theft of intellectual property".

In contrast to minority control, in the U.S., an open accountability in public is and should be the rule. From the New York Times [78],

Defense Secretary Lloyd J. Austin III, who had left the final word on any administrative action, such as reprimands or demotions, to two senior commanders, approved their recommendation not to punish anyone. The two officers . . . found no grounds for penalizing any of the military personnel involved in the strike, said John F. Kirby, the Pentagon's chief spokesman. "What we saw here was a breakdown in process, and execution in procedural events, not the result of negligence, not the result of misconduct, not the result of poor leadership", Mr. Kirby told reporters.

For the future, however, we want to better understand majority rule. Madison [79] was against its inability to protect minorities from out-of-control factions that reduce the freedom of choice, compared to the checks and balances afforded by a republic.

Madison's point is lost on authoritarians, such as China's goal to achieve stability [80],

If all goes to plan for China's Communist Party, 2022 will offer a study in contrasts that humiliates America. China's leaders abhor free elections but they can read opinion polls. They see headlines predicting a drubbing for the Democratic Party in America's mid-term congressional elections in November, condemning the country to the uncertainties of divided government, if not outright gridlock. Should those polls prove accurate, China's propaganda machine will relish a fresh

chance to declare that China enjoys order and prosperity thanks to one-party rule, while American-style democracy brings only chaos, dysfunction and decline.

Equation (1), however, indicates that the news arising from the chaos provides for the opportunities that provide citizens, not central controllers, the information to better adjust to each other, the chaos the source of the innovation and munificence afforded by checks and balances, its lack is the reason why China needs to steal innovation. Regarding thefts, the Department of Defense's audit of its purchases of Commercial Off-the-Shelf (COTS) Items cited cyber-espionage concerns from China [81]:

> [This audit] determined that the DoD purchased and used COTS information technology items with known cybersecurity risks . . . adversaries and malicious actors use [COTS] to introduce cybersecurity vulnerabilities into DoD weapons system and information technology networks that use COTS . . . We recommend that . . . [DoD] develop a risk-based approach . . . to prohibit the purchase and use of high-risk COTS items . . . until mitigation strategies can limit the risk to an acceptable level.

Stealing secrets is a short-term exploitation of a vulnerability. If compulsive, however, if a way of life, the need to steal may become counterproductive. From the title of a new article in the New York Times [82]: "As Beijing Takes Control, Chinese Tech Companies Lose Jobs and Hope". Moreover,

> The crackdown is killing the entrepreneurial drive that made China a tech power and destroying jobs that used to attract the country's brightest . . . The crackdown is killing the innovation, creativity and entrepreneurial spirit that made China a tech power in the past decade. It is destroying companies, profits and jobs that used to attract China's best and brightest.

3.7. Solutions: Cognitive Blindness and Groupthink

Humans have developed two solutions to the quandary posed by uncertainty: use coercion to suppress all but the desired perception, e.g., with consensus-seeking rules that preclude action [16]; or battle test the risk perceptions in a competitive debate between the chosen perception and its competing alternative perceptions, deciding the best with majority rules [14]; e.g., "red teams".

Equation (1) teaches a harsh lesson about the risk perceptions associated with autonomous systems that is strikingly similar to one about quantum mechanics: "There is no such thing as a "true reality" that's independent of the observer; in fact, the very act of making a measurement alters your system irrevocably" [83]. According to Milburn [84], cost–benefit analyses to determine risks may not be formally conducted and published, but the reviews that challenge are the best way to improve risk determination processes and procedures to minimize risks. For example, Justice Ginsburg [45] said that short-circuiting the review process afforded by appeals from lower courts would prevent an "informed assessment of competing interests" (p. 3). The process of challenges laid out by the DOE to recover from the environmental–worker–public risks caused its mismanagement of military nuclear wastes, and by Justice Ginsburg's assessment of competing interests, may ultimately save money, equipment, embarrassment, and morale. The failure to enact such a process is highlighted following the offers of payment as costly compensation made by the U.S. to the families of the drone-strike victims reported by the Wall Street Journal [85]:

> The deaths of the civilians in the August drone strike raised questions about the ability of the U.S. military to conduct from afar "over-the-horizon" counterterrorism operations following the departure of the U.S. troops and their intelligence-gathering capacity. "There's no question that it will be more difficult to identify and engage threats that emanate from the region", Mr. Austin said last month. Former Trump administration national security adviser H.R. McMaster, who served as deputy commander for U.S.-led coalition forces in Afghanistan, told the House Foreign Affairs Committee on October 5, "It is almost impossible

to gain visibility of a terrorist network without partners on the ground who are helping you with human intelligence to be able to map those networks".

In trusting a human–machine system in a high-risk environment, there is always the danger of failure. In the event of a catastrophic failure, such as the case study of the DoD's military drone strike, there is considerable danger that the perceptions of risk may increase to the point that a working weapon system is even precluded from offsetting newly determined risks even when its use is warranted. That is why users of machines (drones) in high-risk environments must take every step to assure success and safety, and to justify the action taken; thus, the recommended use of "red teams" by Said.

4. Conclusions

What many authors often call "AI" is little more than fancy i.i.d. data processors (independent identically distributed). These machine processors are easily fooled (e.g., a Tesla car crashed into side of semi truck), easily manipulated, and easily deceived. Humans, in contrast, live in an interdependent social universe which, presently, machines cannot process, duplicate, nor understand [39]. Can machine intelligence do a lot of damage today? Yes. Can they overtake humans, a worry expressed by Kissinger and colleagues [86]? No.

From the perspective of perceived risks (PRP), for planned operations of autonomous human–machine systems, how rigorous was the assessment of risk (ERP determination)? Was there a test of alternatives? How much uncertainty surrounds the target in the field? Is there, as was found by Said [22] in the tragic drone attack in Afghanistan, a rush to judgment? On the other hand, did the failed drone strike create a barrier to future strikes? Has the decision to launch been justified (e.g., with a red-team assessment)?

Determining risk is already difficult, made more so with the introduction of autonomous systems, especially autonomous human–machine systems. Risk determination needs to be strictly limited in scope to the problem at hand (Said, in [22]). In contrast, unchallenged risk perception can compound the problem of determining risks. An unchallenged risk perception can rise to the point that a human–machine system is no longer used. However, by applying interdependence, a strong process of confrontation in public between a chosen risk perception and its competing alternative can help to hold unfounded risk perceptions in check, uncover deception, and increase innovation. This conclusion was seconded in the journal *Science* [87]. When the stakes are life and death, confrontations test risk determinations and false risk perceptions, allowing the best risk determination to be strengthened and the worst risk perceptions to be rejected. In contrast, suppressing alternative risk perceptions can backfire (e.g., Syria; in [67]).

The breakdown experienced by the DoD affected other organizations allied with the U.S. For example, the U.K. Foreign Office's Secretary Dominic Raab told the BBC that lessons would be learned but the U.K. did a good job compared to other countries. In contrast, signaling an emotional breakdown, a whistleblower, Marshall, has claimed [88],

> The UK Foreign Office's handling of the Afghan evacuation after the Taliban seized Kabul was dysfunctional and chaotic, a whistleblower has said ... [a senior desk officer at the Foreign, Commonwealth and Development Office until resigning in September] said the process of choosing who could get a flight out was arbitrary and thousands of emails with pleas for help went unread. The then Foreign Secretary Dominic Raab was slow to make decisions, he added ... In written evidence to the Foreign Affairs Committee, Mr Marshall said up to 150,000 Afghans who were at risk due to their links to Britain applied to be evacuated-but fewer than 5% received any assistance. "It is clear that some of those left behind have since been murdered by the Taliban", he added.

The last quote introduces an unexpected criticism of our interpretation of the value of majority rule. One of Madison's [79] concerns was the existence of a faction, such as a majority, that exploited an existing minority. It may be that the value of "red teams" is

not only to test the conclusion arrived at by a majority, but to challenge whether or not that risk determination was based on emotion, a disregard for the evidence presented by a situation, or a careful analysis of what is occurring in a situation. Despite this concern, we have shown the value of Equation (1) in several ways: that it justifies the value of tradeoffs; the value of seeking members of a team who best fit together; that spies are aware of this fact and use deception to carry out their misdeeds; that coercion can also produce low structural entropy, thereby reducing the ability of a society to innovate; and that maximum performance arrives by "tuning" the members of a team to perform at their highest levels

Predictions: Future Investigations

Humans are poor at predicting the future (e.g., the inability of Tetlock's well-trained superforecasters to predict both the U.K.'s Brexit departure from Europe and Trump's election to the White House [89]). Applied to the problem of autonomy, specifically human–machine autonomy, a possible solution is to limit the authority of an autonomous team or system. We shall explore this area of research next.

References

1. Pickrell, R. *Nearly 100 Countries Have Military Drones, and It's Changing the Way the World Prepares for War*; Business Insider: New York, NY, USA, 2019.
2. Brynjolfsson, E.; Mitchell, T. What can machine learning do? Workplace implications. *Science* **2017**, *358*, 1530–1534. [CrossRef] [PubMed]
3. Mantica, G. Self-Taught Self-Driving Cars? Available online: https://www.bu.edu/articles/2021/self-taught-self-driving-cars/ (accessed on 30 July 2021).
4. Seetharaman, D.; Horwitz, J.; Scheck, J. Facebook Says AI Will Clean Up the Platform. Its Own Engineers Have Doubts. AI has only minimal success in removing hate speech, violent images and other problem content, according to internal company reports. *Wall Street Journal*, 17 October 2021.
5. Mac, R.; Silverman, C. After The US Election, Key People Are Leaving Facebook And Torching The Company In Departure Notes. A departing Facebook employee said the social network's failure to act on hate speech "makes it embarrassing to work here". *Buzzfeed*, 11 December 2020.
6. Peterson, J.; Bourgin, D.; Agrawal, M.; Reichman, D.; Griffiths, T.L. Using large-scale experiments and machine learning to discover theories of human decision-making. *Science* **2021**, *372*, 1209–1214. [CrossRef]
7. Aikins, M. Times Investigation: In U.S. Drone Strike, Evidence Suggests No ISIS Bomb. U.S. officials said a Reaper drone followed a car for hours and then fired based on evidence it was carrying explosives. But in-depth video analysis and interviews at the site cast doubt on that account. *New York Times*, 3 November 2021.
8. Cooper, H.; Schmitt, E. Pentagon Defends Deadly Drone Strike in Kabul. *New York Times*, 13 December 2021.
9. Tritten, T. Air Force Secretary Taps Watchdog to Weigh Accountability in Botched Kabul Airstrike. Available online: https://www.military.com/daily-news/2021/09/21/air-force-secretary-taps-watchdog-weigh-accountability-botched-kabul-airstrike.html (accessed on 21 September 2021).
10. Doornbus, C. DoD Inspector General Launches Investigation into Kabul Drone Strike that Killed 10 Civilians. Available online: https://www.stripes.com/theaters/us/2021-09-24/kabul-drone-strike-investigation-afghanistan-dod-inspector-general-3005041.html, (accessed on 24 September 2021).
11. Stewart, P.; Ali, I. U.S. Says Kabul Drone Strike Killed 10 Civilians, Including Children, in 'Tragic Mistake'. Available online: https://www.nytimes.com/2021/12/13/us/politics/afghanistan-drone-strike.html (accessed on 13 December 2021).

12. Zengerle, P. U.S. Fallout over Kabul Drone Strike Grows with Plans for Multiple Probes. Available online: https://www.reuters.com/world/asia-pacific/us-fallout-over-kabul-drone-strike-grows-with-plans-multiple-probes-2021-09-23/ (accessed on 23 September 2021).

13. Singh, K. *U.S. Offers Payments, Relocation to Family of Afghans Killed in Botched Drone Attack*; Reuters: London, UK, 2021.

14. Lawless, W.; Akiyoshi, M.; Angjellari-Dajcic, F.; Whitton, J. Public consent for the geologic disposal of highly radioactive wastes and spent nuclear fuel. *Int. J. Environ. Stud.* **2014**, *71*, 41–62. [CrossRef]

15. Slovic, P.; Flynn, J.; Layman, M. Perceived risk, trust, and the politics of nuclear waste. *Science* **1991**, *254*, 1603–1607. [CrossRef] [PubMed]

16. Lawless, W.F.; Bergman, M.; Feltovich, N. Consensus-seeking versus truth-seeking. *ASCE Pract. Period Hazard. Toxic Radioact. Waste Manag.* **2005**, *9*, 59–70. [CrossRef]

17. Paper, W. *European Governance (COM.428 Final)*; Commission of the European Community: Brussels, Belgium, 2001.

18. Rudd, K. Xi Jinping Thought Makes China a Tougher Adversary. *Wall Street Journal*, 12 November 2021.

19. Encyclopedia Britannica. *Command Economy*; Encyclopedia Britannica: Chicag, IL, USA, 2017.

20. Paek, H.J.; Hove, T. Risk Perceptions and Risk Characteristics. In *Oxford Research Encyclopedia of Communication*; Oxford University Press: Oxford, UK, 2017.

21. Brown, V. Risk Perception: It's Personal. *Environ. Health Perspect.* **2014**, *122*, A276–A279. [CrossRef]

22. DoD. *Pentagon Press Secretary John F. Kirby and Air Force Lt. Gen. Sami D. Said Hold a Press Briefing*; Department of Defense: Washington, DC, USA, 2021.

23. CRS. *Defense Primer: Emerging Technologies*; Congressional Research Service: Washington, DC, USA, 2021.

24. Mayes, R. Autonomous Vehicles: Hype or Reality? *Quillette*, 19 October 2021.

25. Jones, E. Major Developments in Five Decades of Social Psychology. In *The Handbook of Social Psychology*; Gilbert, D.T., Fiske, S.T., Lindzey, G., Eds.; McGraw-Hill: New York, NY, USA, 1998; Volume 1, pp. 3–57.

26. Lawless, W. The entangled nature of interdependence. Bistability, irreproducibility and uncertainty. *J. Math. Psychol.* **2017**, *78*, 51–64. [CrossRef]

27. Rudd, J. *Why Do We Think That Inflation Expectations Matter for Inflation? (And Should We?)*; Federal Reserve Board: Washington, DC, USA, 2021.

28. Lawless, W. Quantum-Like Interdependence Theory Advances Autonomous Human–Machine Teams (A-HMTs). *Entropy* **2020**, *22*, 1227. [CrossRef]

29. Jackson, E. How eBay's Purchase of PayPal Changed Silicon Valley. Available online: https://venturebeat.com/2012/10/27/how-ebays-purchase-of-paypal-changed-silicon-valley/ (accessed on 30 October 2012).

30. Dummett, B.; Steinberg, J. CQ Roll Call Owner FiscalNote Strikes SPAC Deal. *Wall Street Journal*, 8 November 2021.

31. Wilmot, S. Driverless 'Robotaxis' Arrive at the Stock Market. Newly listed shares of Aurora Innovation will be a key gauge of investor interest in autonomous vehicles, particularly for private peers Waymo, Cruise and Argo AI. *Wall Street Journal*, 5 November 2021.

32. Fernández-Aráoz, C. Jack Welch's Approach to Leadership. *Harvard Business Review*, 3 March 2020.

33. Board, E. The GE Empire Breaks Up. *Wall Street Journal*, 9 November 2021.

34. Lohr, S.; de la Merced, M. General Electric plans to break itself up into three companies. *New York Times*, 10 November 2021.

35. Baumeister, R.F.; Campbell, J.; Krueger, J.; Vohs, K. Exploding the self-esteem myth. *Sci. Am.* **2005**, *292*, 84–91. [CrossRef]

36. Blanton, H.; Klick, J.; Mitchell, G.; Jaccard, J.; Mellers, B.; Tetlock, P. Strong Claims and Weak Evidence: Reassessing the Predictive Validity of the IAT. *J. Appl. Psychol.* **2009**, *94*, 567–582. [CrossRef] [PubMed]

37. Hagger, M.; Chatzisarantis, N.; Alberts, H.; Anggono, C.O.; Batailler, C.; Birt, A.R.; Brandt, J.; Brewer, G.; Bruyneel, S.; Calvillo, D.P.; et al. A Multilab Preregistered Replication of the Ego-Depletion Effect. *Perspect. Psychol. Sci.* **2016**, *11*, 546–573. [CrossRef]

38. Nosek, B. Estimating the reproducibility of psychological science. *Science* **2015**, *349*, 943.

39. Schölkopf, B.; Locatello, F.; Bauer, S.; Ke, N.R.; Kalchbrenner, N.; Goyal, A.; Bengio, Y. Towards Causal Representation Learning. *arXiv* **2021**, arXiv:2102.11107.

40. Crandall, C.; Eshleman, A.; O'Brien, L. Social Norms and the Expression and Suppression of Prejudice: The Struggle for Internalization. *J. Personal. Soc. Psychol.* **2002**, *82*, 359–378. [CrossRef]

41. Leach, C. *Journal of Personality and Social Psychology: Interpersonal Relations and Group Processes*; American Psychological Association: Washington, DC, USA, 2021.

42. Mann, R. Collective decision making by rational individuals. *Proc. Natl. Acad. Sci. USA* **2018**, *115*, E10387–E10396. [CrossRef] [PubMed]

43. Weinberg, S. The Trouble with Quantum Mechanics. *The New York Review of Books*. 2017. Available online: http://www.nybooks.com (accessed on 1 February 2022).

44. Martinez, M.; Sequoiah-Grayson, S. Logic and Information. In *The Stanford Encyclopedia of Philosophy*; Edward, N.Z., Ed.; Stanford University Press: Redwood City, CA, USA, 2019.

45. Ginsburg, R. *American Electric Power co., Inc. et al v. Connecticut et al.*; US Supreme Court: Washington, DC, USA, 2011; pp. 10–174.

46. Pinker, S. *Rationality: What It Is, Why It Seems Scarce, Why It Matters*; Viking Press: New York, NY, USA, 2021.

47. Thagard, P. Rationality and science. In *Handbook of Rationality*; Mele, A., Rawlings, P., Eds.; Oxford University Press: Oxford, UK, 2004; pp. 363–379.

48. Wilson, E. *Consilience: The Unity of Knowledge*; Vintage Books: New York, NY, USA, 1998.
49. Ponce de León, M.; Bienvenu, T.; Marom, A.; Engel, S.; Tafforeau, P.; Alatorre Warren, J.L.; Kurniawan, I.; Murti, D.B.; Suriyanto, R.A.; Koesbardiati, T.; et al. The primitive brain of early Homo. *Science* **2021**, *372*, 165–171. [CrossRef] [PubMed]
50. Shannon, C. A Mathematical Theory of Communication. *Bell Syst. Tech. J.* **1948**, *27*, 379–423, 623–656. [CrossRef]
51. Augier, M.; Barrett, S. *General Anthony Zinni (ret.) on Wargaming iraq, Millennium Challenge, and Competition*; Center for International Maritime Security: Washington, DC, USA, 2021.
52. Luttwak, E. How the CIA Lets America Down. 'Counterinsurgency warfare' is a nullity without human intelligence. *Wall Street Journal*, 14 November 2021.
53. Mattioli, D. Amazon Scooped Up Data From Its Own Sellers to Launch Competing Products. Contrary to assertions to Congress, employees often consulted sales information on third-party vendors when developing private-label merchandise. *Wall Street Journal*, 23 April 2020.
54. Mattioli, D. Members of Congressional Committee Question Whether Amazon Executives Misled Congress. In a letter, bipartisan group of representatives asks for documents, 'exculpatory' evidence as they consider whether to recommend Justice Department investigation. *Wall Street Journal*, 18 October 2021.
55. Lawless, W.; Mittu, R.; Moskowitz, I.; Sofge, D.; Russell, S. *Cyber-(In)security, Revisited: Proactive Cyber-Defenses, Interdependence and Autonomous Human-Machine Teams*; Springer Nature: Berlin, Germany, 2020.
56. Trofimov, Y.; Stancati, M. Taliban Covert Operatives Seized Kabul, Other Afghan Cities From Within. Success of Kabul's undercover network, loyal to the Haqqanis, changed balance of power within Taliban after U.S. withdrawal. *Wall Street Journal*, 28 November 2021.
57. Robison, P. *Flying Blind. The 737 MAX Tragedy and the Fall of Boeing*; Doubleday: New York, NY, USA, 2021.
58. Galle, A. Drinking from the Fetid Well: Data Poisoning and Machine Learning. *US Nav. Inst. Proc.* **2022**, *148*, 1427.
59. Zegart, A. *Spies, Lies, and Algorithms: The History and Future of American Intelligence*; Princeton University Press: Princeton, NJ, USA, 2022.
60. Bergman, R.; Mazzetti, M. The Battle for the World's Most Powerful Cyberweapon. A Times investigation reveals how Israel reaped diplomatic gains around the world from NSO's Pegasus spyware—A tool America itself purchased but is now trying to ban. *New York Times Magazine*, 31 January 2022.
61. Hein, B. Lawmakers Plan to Tank the Startup Economy. A measure aimed at big tech would curb innovation, risk-taking and entrepreneurship by small companies. *Wall Street Journal*, 18 October 2021.
62. Mickle, T. Google CEO Sundar Pichai Calls for Government Action on Cybersecurity, Innovation. Executive urges governments to adopt a Geneva Convention for cybersecurity, and for the U.S. to invest more in tech. *Wall Street Journal*, 18 October 2021.
63. Keynes, J.M. *The General Theory of Employment, Interest and Money*; Macmillan: New York, NY, USA, 1936; pp. 161–162.
64. Akerlof, G.A.; Shiller, R.J. *Animal Spirits: How Human Psychology Drives the Economy, and Why It Matters for Global Capitalism*; Princeton University Press: Princeton, NJ, USA, 2009.
65. Roach, S. *China's Animal Spirits Deficit*; Project Syndicate: Prague, Czech Republic, 2021.
66. Phillips, D.; Schmitt, E. How the U.S. Hid an Airstrike That Killed Dozens of Civilians in Syria? The military never conducted an independent investigation into a 2019 bombing on the last bastion of the Islamic State, despite concerns about a secretive commando force. *New York Times*, 15 November 2021.
67. Brest, M. US admits to strikes that killed civilians in Syria years ago. *Washington Examiner*, 15 November 2021.
68. Phillips, D.; Schmitt, E.; Mazzetti, M. Civilian Deaths Mounted as Secret Unit Pounded ISIS. An American strike cell alarmed its partners as it raced to defeat the enemy. *New York Times*, 27 December 2021.
69. Chin, J. Xi Jinping's Leadership Style: Micromanagement That Leaves Underlings Scrambling. Chinese president delves into the details of policy and sometimes issues cryptic instructions that officials go overboard trying to carry out. *Wall Street Journal*, 15 December 2021.
70. James, C. *Victims and Bullies: Understanding the Optics of Coercion in a New Era of Us Foreign Policy*; Modern War Institute: West Point, NY, USA, 2021.
71. Hoffmann, B. The international dimension of authoritarian regime legitimation: Insights from the Cuban case. *J. Int. Relat. Dev.* **2015**, *18*, 556–574. [CrossRef]
72. Beech, H. They Warned Their Names Were on a Hit List. *New York Times*, 14 November 2021.
73. Rockoff, J.; Loftus, P. Johnson and Johnson to Split Consumer From Pharmaceutical, Medical-Device Businesses, Creating Two Companies. *Wall Street Journal*, 12 November 2021.
74. Atlamazoglou, S. Why America Never Sold the f-22 Raptor to Foreign Countries. Available online: https://www.sandboxx.us/blog/why-america-never-sold-the-f-22-raptor-to-foreign-countries/ (accessed on 15 November 2021).
75. Marson, J.; Legorano, G. China Bought Italian Military-Drone Maker Without Authorities' Knowledge. Sale illustrates Europe's weak rules on purchases of sensitive technology. *Wall Street Journal*, 15 November 2021.
76. Wong, C.; Zhai, K. How Xi Jinping Is Rewriting China's History to Put Himself at the Center? The full text of a resolution on the Communist Party's 100-year history portrays the Chinese leader as uniquely suited to continue Mao's revolutionary project. *Wall Street Journal*, 17 November 2021.
77. Duesterberg, T. The Slow Meltdown of the Chinese Economy. Beijing's troubles are an opportunity for the U.S.—If Washington can recognize it. *Wall Street Journal*, 20 December 2021.

78. Schmitt, E. No U.S. Troops Will Be Punished for Deadly Kabul Strike, Pentagon Chief Decides. The military initially defended the strike, which killed 10 civilians including seven children, but ultimately called it a tragic mistake. *New York Times*, 13 December 2021.

79. Madison, J.P. The Union as a Safeguard Against Domestic Faction and Insurrection. To the people of New York. In *Federalist Papers: No. 10*; Lillian Goldman Law Library: New Haven, CT, USA, 1787.

80. Rennie, D. China hopes to flaunt the merits of its political system over America's. The Communist Party congress will contrast with America's mid-term elections. *The Economist*, 8 November 2021.

81. Audit, D. Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items DODIG-2019-106. Available online: https://www.oversight.gov/report/dod/audit-dod (accessed on 30 July 2019).

82. Yuan, L. As Beijing Takes Control, Chinese Tech Companies Lose Jobs and Hope. The crackdown is killing the entrepreneurial drive that made China a tech power and destroying jobs that used to attract the country's brightest. *New York Times*, 12 January 2022.

83. Siegel, E. Ask Ethan: What Should Everyone Know about Quantum Mechanics? Available online: https://bigthink.com/starts-with-a-bang/basics-quantum-mechanics/ (accessed on 29 October 2021).

84. Milburn, A. Drone Strikes Gone Wrong: Fixing a Strategic Problem. *Small Wars Journal*, 8 October 2021.

85. Nasaw, D. U.S. Offers Payments to Families of Afghans Killed in August Drone Strike. State Department to support slain aid worker's family's effort to relocate to U.S., Pentagon says. *Wall Street Journal*, 13 December 2021.

86. Kissinger, H.; Schmidt, E.; Huttenlocher, D. The Challenge of Being Human in the Age of AI. Reason is our primary means of understanding the world. How does that change if machines think? *Wall Street Journal*, 1 November 2021.

87. Avin, S.; Belfield, H.; Brundage, M.; Krueger, G.; Wang, J.; Weller, A.; Anderljung, M.; Krawczuk, I.; Krueger, D.; Lebensold, J.; et al. Filling gaps in trustworthy development of AI. *Science* **2021**, *374*, 1327–1329. [CrossRef] [PubMed]

88. Landale, J.; Lee, J. Afghanistan: Foreign Office chaotic during Kabul evacuation-whistleblower. *BBC News*, 7 December 2021.

89. Tetlock, P.; Gardner, D. *Superforecasting: The Art and Science of Prediction*; Crown Publishers: New York, NY, USA, 2015.