Resilience: A New Tool in the Risk Governance Toolbox for Emerging Technologies

Gary E. Marchant[†*] *& Yvonne A. Stevens*[**]

Emerging technologies like nanotechnology, synthetic biology, artificial intelligence, and many others present significant governance challenges. These challenges include highly uncertain benefits, risks, and trajectories associated with the technology, an extremely rapid pace of development and change, and a broad range of applications that implicate many different industries, regulatory agencies, and stakeholders. Traditional ex ante risk management approaches such as risk analysis and precaution have struggled to provide adequate governance of such technologies, in large part because of the difficulty in predicting in advance realistic risk scenarios. In the article, we propose a different approach that shifts much of the governance task and burden from the traditional ex ante approaches of risk analysis and precaution to focus more on the ex post strategy of resilience. Resilience seeks to minimize the harm from a bad outcome, and offers many potential advantages for dealing with emerging technologies with highly uncertain risks that cannot be predicted in advance. There are a number of potential resilience measures that could be used to help govern many emerging technologies — we identify and describe many such measures and define two categories. Procedural resilience measures put in place a decision-making process that will allow for more reflexive and adaptive decision-making, thereby facilitating early detection and

 This article was initially developed as a policy paper for, and with an honorarium from, the University of Texas at Austin Center for Politics and Government. The authors express their appreciation for the helpful suggestions from Dima Shamoun and two anonymous reviewers.

* Regents' Professor and the Lincoln Professor of Law, Ethics & Emerging Technologies at the Sandra Day O'Connor College of Law at Arizona State University ("ASU"), and Faculty Director of the Center for Law, Science & Innovation at ASU.

** Faculty Fellow of the Center for Law, Science & Innovation, and on the full-time faculty of the Sandra Day O'Connor College of Law at ASU.

response to adverse effects. Substantive resilience measures put in place strategies, back-up plans, and resources that can help minimize harms when adverse effects occur. A resilience strategy that incorporates a mix of procedural and substantive resilience measures may help to ensure the tremendous potential benefits of emerging technologies are realized while also minimizing any adverse impacts from such technologies.

TABLE OF CONTENTS

The governance of emerging technologies such as nanotechnology, synthetic biology, artificial intelligence/robotics, CRISPR gene editing, and applied neuroscience has focused largely on a contest between two *ex ante* risk management approaches: (1) risk analysis and (2) precaution. Risk analysis attempts to utilize available scientific information to quantify the risks of a technology in advance ("risk assessment"), and then to put in place preventive measures to reduce those risks to an acceptable or cost-effective level ("risk management"). Precaution, often applied in one form or another, as the "precautionary principle," recognizes the inherent uncertainties in many risk decisions and errs on the side of safety by restricting a technology until it has been demonstrated to be sufficiently safe. These *ex ante* risk management approaches can be applied to a technology wholesale, or more narrowly to any specific application of the technology.

Both risk analysis and precaution have their strengths and weaknesses for governance of emerging technologies. Indeed, most risk management decisions incorporate some elements of risk analysis and precaution, although the relative weight given to risk analysis and precaution varies between decision-makers and decisions. For example, a decision based on risk analysis often incorporates upper-bound estimates of some risk components to deal with uncertainties, an inherent form of precaution.[1] And most precautionary decisions incorporate some elements of risk assessment in order to obtain a sense of scale and priority of risks that should be subject to precautionary decisions.[2]

Notwithstanding some benefits of both approaches, there is lack of consensus and dissatisfaction with the capability of these two traditional risk management approaches to ensure safe development of emerging technologies without unduly suppressing their benefits. Both the risk analysis and precaution approaches exercise *ex ante* risk governance — attempting to anticipate and prevent risks before they occur. But there is also the potential and need for *ex post* governance — attempting to mitigate or minimize, sometimes inevitable, harm

[1] *See* Adam M. Finkel, *The Case for "Plausible Conservatism" in Choosing and Altering Defaults*, *in* NAT'L RESEARCH COUNCIL, SCIENCE AND JUDGMENT IN RISK ASSESSMENT 601-27 (1994).

[2] *See* COMM'N OF THE EUROPEAN COMMUNITIES, COMMUNICATION FROM THE COMMISSION ON THE PRECAUTIONARY PRINCIPLE 13-14 (Feb. 2, 2000), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0001&from=EN ("An assessment of risk should be considered where feasible when deciding whether or not to invoke the precautionary principle.").

after it occurs. The best known *ex post* approach to governance is liability. But recently, another important *ex post* governance tool has arisen — resilience.[3] Resilience is the capacity of a system to recover after harm has occurred. While there has been some confusion in the literature about whether risk analysis is part of resilience or resilience is part of risk analysis, the two approaches are distinct but complementary.[4]

This paper examines the role of resilience in governance of emerging technologies, and shows how this concept can buttress and help relieve the burdens and shortcomings of risk analysis, precaution, and liability. Instead of hopelessly trying to anticipate and quantify unascertainable future risks associated with emerging technologies, resilience relies on a trial-and-error approach that seeks to aggressively explore the potential benefits of a new technology while remaining vigilant and ready to respond to any emerging harms, an approach described by the political scientist Aaron Wildavsky as "searching for safety."[5] Both the risks and benefits of emerging technologies are not readily apparent — they can only be discovered through trial and error. Resilience seeks to provide protection when the trials encounter danger. Resilience is also in conformance with the "learning by doing" approach of adaptive management.[6]

An optimal governance strategy should consider both the risks and benefits of an emerging technology, and employ a mix of these four risk governance tools, mixing and matching depending on the context and stakes. In particular, if a sound and effective resilience system is in place, less precaution may be needed in going forward with a potentially beneficial emerging technology.

Part I of this paper proposes an integrated governance framework that incorporates both *ex ante* and *ex post* approaches, built on the four governance tools of risk analysis, precaution, liability, and resilience. It identifies the strengths and weaknesses of all four of these governance methods, and shows how an optimal technology governance system should integrate and balance the four tools based

[3] Although resilience approaches are *ex post* in that they apply after harm has occurred, such strategies often need to be planned in advance — sometimes referred to as "resilience by design." JOSEPH FIKSEL, RESILIENT BY DESIGN 19-34 (2015); *see also infra* note 37 and accompanying text.

[4] *See infra* notes 49-51 and accompanying text.

[5] AARON WILDAVSKY, SEARCHING FOR SAFETY 228 (1988) (explaining that safety is not "a ripe fruit waiting only to be plucked," but rather a condition that "results from a process of discovery").

[6] Eric Biber, *Adaptive Management and the Future of Environmental Law*, 46 AKRON L. REV. 933, 934 (2013).

on the context and stakes of the governance decision. Part II delves into resilience in more detail, explaining the history and often confused meaning of the concept of resilience, as well as the potential advantages it offers for the safe development and implementation of emerging technologies. Part III then describes procedural and substantive resilience governance tools that could apply to emerging technologies.

I. TECHNOLOGY GOVERNANCE FRAMEWORKS

Emerging technologies such as nanotechnology, synthetic biology, artificial intelligence/robotics, CRISPR gene editing, and applied neuroscience present significant governance challenges.[7] The benefits and risks of these technologies are highly uncertain, but either or both could be substantial. The technologies are advancing at a very rapid pace, perhaps too fast for traditional regulatory programs to keep pace. These technologies often present benefits and risks beyond the conventional environmental, health and safety realms that agencies are used to regulating, such as concerns relating to ethics, socio-economic impacts, distributional issues, human enhancement, privacy, and other concerns. Finally, today's evolving technologies are being applied by many different industries for different purposes, presenting different risks, benefits, and regulatory jurisdictions.

A. Ex Ante *Approaches*

Two competing risk management frameworks have dominated the debate on governance of these emerging technologies to date. Both of these frameworks use an *ex ante* approach — they attempt to anticipate and put into place policies to prevent harms from occurring before the technology is implemented. The first framework is risk analysis, which attempts to use available scientific information to estimate risks and then apply various risk management decision rules to reduce the risks to acceptable or efficient levels. The second approach is precaution, which applies a more stringent risk management approach that seeks to delay or restrict new technologies until they have been demonstrated to be safe. As discussed below, both risk analysis and precaution are *ex ante* risk management tools

[7] *See* Gary E. Marchant, *Conclusion: Emerging Governance for Emergent Technologies*, *in* INNOVATIVE GOVERNANCE MODELS FOR EMERGING TECHNOLOGIES 254-58 (Gary E. Marchant et al. eds., 2013); Gary E. Marchant & Wendell Wallach, *Introduction*, *in* EMERGING TECHNOLOGIES: ETHICS, LAW AND GOVERNANCE 1-12 (Gary E. Marchant & Wendell Wallach eds., 2016).

that have relevance for the governance of emerging technologies, but both have significant limitations.

1. Risk Analysis

Risk analysis uses the best available scientific information to estimate potential risks, a step known as risk assessment, and then applies a risk management approach, such as acceptable risk analysis, cost-benefit analysis, cost-effectiveness analysis, or feasibility analysis to reduce these estimated risks to acceptable or efficient levels. The biggest strength of the risk analysis paradigm is that it attempts to do the best job possible to measure exactly the appropriate concerns — i.e., what the actual risks are — and then use structured decision rules to reduce those risks to the optimal levels. There are innumerable known, probable, and possible risks associated with any technology or product, and the magnitude and frequency of these risks varies dramatically across different technologies, applications, and products. Risk analysis provides a common currency for comparing and prioritizing risks,[8] given the reality that not all risks can or should be eliminated, especially when some risks are associated with significant known or potential benefits. Because it focuses on the questions that are most directly relevant, risk analysis is the favored risk management approach used by most regulatory agencies.[9]

The biggest weakness of traditional risk analysis is the gaps and uncertainties in the data upon which the risk assessment is derived.[10] These gaps and uncertainties are addressed using assumptions that often assume a plausible upper bound of risk.[11] However, there are often disputes and controversies about which assumptions are used, and whether they are over-protective or under-predictive. Choices about what assumptions are used in a risk assessment can change the final risk estimate by several orders of magnitude or more.[12] In the

[8] *See* NAT'L RESEARCH COUNCIL, SCIENCE AND JUDGMENT IN RISK ASSESSMENT 17 (1994) ("Quantitative risk assessment is attractive because, at least ideally, it allows decision-makers and the public to discriminate between important and trivial threats (thus going beyond qualitative findings that there is some risk, however small).").

[9] *See* NAT'L RESEARCH COUNCIL, RISK ASSESSMENT IN THE FEDERAL GOVERNMENT: MANAGING THE PROCESS 40-48 (1983).

[10] *See id.* at 11 ("The dominant analytic difficulty is pervasive uncertainty."); NAT'L RESEARCH COUNCIL, SCIENCE AND DECISIONS: ADVANCING RISK ASSESSMENT 97 (2009) ("Uncertainty is foremost among the recurring themes in risk assessment.").

[11] *See* NAT'L RESEARCH COUNCIL, *supra* note 9, at 36-37.

[12] *See, e.g.*, Emmanuel Somers, *Perspectives on Risk Management*, 15 RISK ANALYSIS 677, 680 (1995) (depending on assumptions used, risk estimates for furans and

case of emerging technologies, the uncertainties and limitations go beyond missing data and include the lack of validated methods to define, characterize, measure, and quantify emerging technologies such as nanomaterials.[13] For emerging technologies, which produce greater uncertainties than many other regulated products with regard to both their benefits and risks, the problem of how to address uncertainty is an even bigger concern.

For example, estimating the toxicity of nanomaterials is much more difficult as compared to traditional chemicals. Tools like quantitative structure-activity relationship ("QSAR") models, which provide quite reliable risk estimates for common chemicals, do not work for most nanomaterials. This is due to the fact that nanomaterials' toxicity is influenced by factors other than chemical structure, including size, surface area, surface properties, and other factors.[14] In addition to the greater uncertainty in calculating known risks, emerging technologies will sometimes present "surprises" consisting of risks that were not even anticipated, sometimes referred to as "unknown unknowns" (also sometimes referred to as "black swans" or "Type III" risks).[15] These challenges limit the utility of risk analysis for many emerging technologies.

2. Precaution

The primary risk management competitor to traditional risk analysis is precaution, most commonly expressed as the precautionary principle.[16] Although risk analysis often provides some degree of precaution when it uses plausible upper-bound assumptions, the precautionary principle is based on the belief that additional

dioxins based on the same experimental evidence can differ by 1600-fold).

[13] *See* EPA, NANOTECHNOLOGY WHITE PAPER 72-73 (2007), https://archive.epa.gov/osa/pdfs/web/pdf/epa-nanotechnology-whitepaper-0207.pdf.

[14] *See* David W. Hobson et al., *Applied Nanotoxicology*, 35 INT'L J. TOXICOLOGY 5, 6 (2016).

[15] Terje Aven, *Implications of Black Swans to the Foundations and Practice of Risk Assessment and Management*, 134 RELIABILITY ENGINEERING & SYS. SAFETY 83, 84-86 (2015); NASSIM NICHOLAS TALEB, THE BLACK SWAN: THE IMPACT OF THE HIGHLY IMPROBABLE xxii-xxiii (2d ed. 2010).

[16] Although there is no single or official definition of the precautionary principle, one of the most influential definitions and arguments for the precautionary principle was a statement produced by supporters of the principle who convened at the Wingspread conference center in Wisconsin in January 1998 to better define and operationalize the precautionary principle. *See The Wingspread Statement on the Precautionary Principle*, SCI. & ENVTL. HEALTH NETWORK (Jan. 26, 1998), http://sehn.org/wingspread-conference-on-the-precautionary-principle.

protections are needed against uncertain risks. Some formulations of the precautionary principle utilize traditional risk assessment but then just apply a more protective risk management approach.[17] Other formulations believe that scientific assessment of risk is too uncertain to provide a satisfactory basis for regulatory decisions and therefore should be disregarded.[18] Accordingly, the precautionary principle applies a more stringent risk management approach that assumes a new technology or activity cannot be authorized until it has been affirmatively demonstrated to be safe.[19] The core idea behind the precautionary principle is "better safe than sorry,"[20] which certainly has some relevance especially for emerging technologies that could present catastrophic and even existential risks. The precautionary principle has been adopted into many laws in the European Union and some other jurisdictions, and has been incorporated into dozens of international environmental treaties, but has achieved relatively little legal recognition in the United States.[21]

The precautionary principle suffers from some serious flaws, at least as applied to date.[22] There are multiple different interpretations and versions of the precautionary principle, differing in fundamental

[17] *See* COMM'N OF THE EUROPEAN COMMUNITIES, *supra* note 2, at 13 ("Before the precautionary principle is invoked, the scientific data relevant to the risks must first be evaluated.").

[18] *See* D. Santillo et al., *The Precautionary Principle: Protecting Against Failures of Scientific Method and Risk Assessment*, 36 MARINE POLLUTION BULL. 939, 946-48 (1998).

[19] *See* SCI. & ENVTL. HEALTH NETWORK, *supra* note 16 ("[T]he proponent of an activity, rather than the public, should bear the burden of proof.").

[20] *See* Cass R. Sunstein, *Beyond the Precautionary Principle*, 151 U. PA. L. REV. 1003, 1004 (2003).

[21] *See* Scott LaFranchi, *Surveying the Precautionary Principle's Ongoing Global Development: The Evolution of an Emergent Environmental Management Tool*, ENVTL. AFF. 679, 683-99 (2005).

[22] There is a wide range of interpretations of the precautionary principle, some more extreme than others. Some anti-technology organizations assert that the precautionary principle requires bans or moratoria on many emerging technologies. *See, e.g.*, FRIENDS OF THE EARTH ET AL., THE PRINCIPLES FOR THE OVERSIGHT OF SYNTHETIC BIOLOGY 3 (2012), http://www.etcgroup.org/sites/www.etcgroup.org/files/The%20Principles%20for%20the%20Oversight%20of%20Synthetic%20Biology%20FINAL.pdf. Such extreme constructions of the precautionary principle effectively put a permanent roadblock in the way of emerging technologies, since without any opportunity for commercialization there will be no opportunity to learn about the technology and no incentive to invest in such technologies. More reasonable interpretations of the precautionary principle are also advanced, in which a technology is allowed to proceed cautiously in a step-wise function, but with the intention to allow the technology to be deployed safely if that is possible. *See, e.g.*, Gregory E. Kaebnick et al., *Precaution and Governance of Emerging Technologies*, 354 SCIENCE 710, 711 (2016).

respects in how the principle is applied.[23] Most proponents of the precautionary principle, both in governments and in advocacy organizations, have resisted defining key questions about the precautionary principle — such as, what is the level of uncertainty or indicators of risk sufficient to trigger the precautionary principle, and what is required to satisfy the precautionary principle to allow a technology or product to go forward?[24] Perhaps the most fundamental problem with the precautionary principle is that it usually fails to acknowledge the risks of *not* implementing a technology.[25] Many emerging technologies provide potential health, environmental, and safety benefits which are foregone if technologies are blocked because of their possible risks. Thus, the precautionary principle creates the risk of doing more harm than good.[26]

While both risk analysis and precaution have an important role to play in an integrated risk management framework for emerging technologies, they, alone or together, fail to provide satisfactory governance for most emerging technologies. This creates a potential role for *ex post* approaches to help fill the governance gaps.

B. Ex Post *Approaches*

Given the almost impossible challenge of trying to fully anticipate the risks of emerging technologies using *ex ante* approaches, *ex post* strategies may have increased saliency. *Ex post* governance approaches have the advantage of not having to anticipate potential risks, but rather having to respond to such risks after they have manifested. (Of course, when the likely risks are serious and irreversible, the case is much stronger for *ex ante* precautionary regulation.) *Ex post* approaches thus avoid the resources, uncertainties, and controversies inherent in *ex ante* approaches,[27] and in particular avoid the need to address speculative risks that turn out to never manifest. Liability is

[23] *See generally* Per Sandin, *Dimensions of the Precautionary Principle*, 5 HUMAN ECOLOGY RISK ASSESS. 889 (1999) (demonstrating major differences in nineteen different formulations of the precautionary principle).

[24] *See* Gary E. Marchant, *From General Policy to Legal Rule: Aspirations and Limitations of the Precautionary Principle*, 111 ENVTL. HEALTH PERSP. 1799, 1799-1803 (2003).

[25] *See* Sunstein, *supra* note 20, at 1020-23.

[26] Frank B. Cross, *Paradoxical Perils of the Precautionary Principle*, 53 WASH. & LEE L. REV. 851, 860-61 (1996).

[27] Resilience does involve some anticipatory preparations, but the actual implementation of the resilience measures, which is most resource-consuming, is not triggered until actual harm occurs. *See infra* note 37 and accompanying text.

the traditional *ex post* approach, but resilience provides another *ex post* strategy.

1. Liability

Liability has always played an important role in the American approach to product and process safety. For products such as asbestos, tobacco, and cellular phones, liability has been the dominant governance strategy, with *ex ante* regulation playing a secondary or even insignificant contribution. Liability offers several advantages as a governance approach.[28] It most often does not rely on speculative models and assumptions about what risks a product may present, but rather focuses only on harms that have actually occurred (with the exception of latent tort claims.)[29] It therefore does not suppress products that turn out not to cause undue harm, which is a problem with *ex ante* approaches, especially those based on the precautionary principle.[30] Liability also compensates those who have been injured, unlike *ex ante* approaches, which provide no remedy if harm occurs. Liability can also provide a powerful deterrent for manufacturers, exerting powerful economic pressure for safer products.

However, liability also has its limitations and shortcomings as a technology governance. First, causation is often a problem in allocating liability, especially for exotic technologies such as nanotechnology and synthetic biology without known hazard potentials. Uncertainty about causation, or not being able to meet the requisite legal standard of proof, can result in some harms going uncompensated when causation cannot be sufficiently demonstrated,

[28] For arguments in favor of liability as a regulatory tool from a variety of different political perspectives, see TERRY L. ANDERSON & DONALD R. LEAL, FREEMARKET ENVIRONMENTALISM 184-85 (Rev. Ed. 2001); Jonathan H. Adler, *Free and Green: A New Approach to Environmental Protection*, 24 HARV. J.L. & PUB. POL'Y 653, 667-71 (2001); Keith N. Hylton, *When Should We Prefer Tort Law to Environmental Regulation?*, 41 WASHBURN L.J. 515, 520-28 (2002); Alexandra B. Klass, *Common Law and Federalism in the Age of the Regulatory State*, 92 IOWA L. REV. 545, 582-84 (2007).

[29] Latent tort claims are claims for increased risk of injury, fear of cancer, and medical monitoring, where plaintiffs may have been exposed to a hazardous agent but have not yet manifested clinical disease. *See* James Pizzirusso, Note, *Increased Risk, Fear of Disease and Medical Monitoring: Are Novel Damage Claims Enough to Overcome Causation Difficulties in Toxic Torts*, 7 ENVTL. LAWYER 183, 197-204 (2001).

[30] James A. Henderson, Jr., *Tort vs. Technology: Accommodating Disruptive Innovation*, 47 ARIZ. ST. L.J. 1145, 1147 (2015) ("American tort law, including products liability, contains a number of features that reveal the system generally to be conducive to the introduction and promotion of disruptively creative, albeit dangerous, new technology.").

but can also result in the manufacturers or distributors of some products (e.g., silicone breast implants) being unjustly found liable for harms they did not in fact cause. For very dangerous products, liability can often be insufficient, as demonstrated by the massive pain, suffering, and deaths suffered by hundreds of thousands of workers who developed mesothelioma from asbestos exposure. Monetary awards, while justified, fail to adequately compensate the victims and their families for their losses, and, in retrospect, a preventive *ex ante* approach would be far superior. Another problem with liability is that an entity that causes injury may be judgment proof — for example, it may be a small start-up with limited resources unable to compensate the injuries it caused, or it may be bankrupt by the time an injury manifests and liability claims are ready to be filed in court.[31]

Take nanotechnology as an example. Suppose that an individual suffers lung damage from breathing in carbon nanotubes. The plaintiff would face insurmountable challenges in bringing a successful tort suit.[32] First, many different manufacturers and product formulators manufacture or use carbon nanotubes in their products — it would be difficult for a plaintiff to know which product and company was responsible for the carbon nanotubes that caused their lung damage. Second, the plaintiff would have the burden of proof to demonstrate causation using scientific evidence that can satisfy the strict admissibility tests the courts apply to such evidence. There are no human epidemiology studies of carbon nanotubes at this time (too soon after market entry), which is the preferred type of evidence courts require to prove causation. Even animal studies are few in number, small in size, and give mixed results, and would almost certainly not support a causation claim. Finally, the lung effects of the nanotubes may take decades to manifest, by which time the manufacturer may have gone out of business, the evidence of exposure may have gone stale, and the statute of limitations may have run. For all these reasons, tort liability is unlikely to be a very effective remedy for harms caused by emerging technologies such as nanotechnology, undermining both the compensation and deterrence goals of liability.

Thus, liability, like risk analysis and precaution, may play an important and essential role in the governance framework for

---

[31] David A. Dana & Hannah J. Wiseman, *A Market Approach to Regulating the Energy Revolution: Assurance Bonds, Insurance, and the Certain and Uncertain Risks of Hydraulic Fracturing*, 99 IOWA L. REV. 1523, 1557 (2014).

[32] *See* Edward R. Glady, Jr. et al., *Nanotechnology Liability: Do We Steer or Just Go Along for the Ride?*, 52 JURIMETRICS 313, 324-25 (2012).

emerging technologies in some cases, but alone or together with the *ex ante* approaches, is not able to provide optimal risk governance.

2. Resilience

Resilience is the fourth and least developed technology governance tool. Resilience has been defined by the U.S. National Academies as "the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events."[33] Resilience, like liability, is therefore *ex post*, in that it seeks to minimize the extent and duration of harm after failure or injury has occurred. Unlike liability, resilience can be planned for *ex ante* before damage has occurred; yet, like liability, is only implemented *ex post*.[34] Examples of such "resilience by design," discussed in more detail below,[35] are monitoring programs that seek the earliest possible detection of harm occurring, redundant systems that can kick in when primary safety systems fail, and "kill switches" that can disable a technology that is causing harm. Although these resilience tools are put into place *ex ante*, they are designed to minimize harms only after a malfunction or hazard has occurred. To give a practical, well-known example, software developers will often release beta or early versions of their software programs that they know will contain bugs, but will then actively seek user feedback to identify and fix glitches in the software code.[36]

Resilience has two key advantages over other technology governance approaches. First, because it is *ex post*, it can be based on real risks and harms, rather than speculative risks that are estimated *ex ante*.[37] Second, because it is permissive rather than prohibitive, resilience

[33] THE NAT'L ACADEMIES, DISASTER RESILIENCE: A NATIONAL IMPERATIVE 1 (2012).

[34] It is worth noting that in certain instances, liability may take the form of resilience, especially in the context of damages claims that require making the injured persons "whole" again, such that the line between liability and resilience as *ex post* governance tools, is slightly blurred. Nonetheless, generally speaking, we view liability and resilience as distinct concepts and, therefore, present them as such in the present discussion.

[35] *See infra* Section III.

[36] We thank Dima Shamoun for this example.

[37] Nobel Prize winning co-discoverer of the DNA double-helix expressed such a view in looking back at the initial restrictions put on beneficial recombinant DNA research in the 1970s based on only hypothetical risks: "The moral I draw from this painful episode is this: Never postpone experiments that have clearly defined future benefits for fear of dangers that can't be quantified. Though it may sound at first uncaring, we can react rationally only to real (as opposed to hypothetical) risks." James D. Watson, *All for the Good: Why Genetic Engineering Must Soldier On*, TIME, Jan. 11, 1999, at 91.

favors going forward with technologies for which there is public or industrial demand, providing a form of "permissionless innovation" with some assurance of safety.[38] As such, resilience holds much promise for playing a greater role in the governance of emerging technologies, which is the focus of the remainder of this paper.

The four principal tools of technology governance are illustrated in Figure 1 — and are distinguished based on whether they are *ex ante* versus *ex post*, and permissive versus prohibitive. Each of the four governance approaches will have some relevance for any risk management decision, with the relative weight given to any particular tool in a given context dependent on the strengths and weaknesses of each of the other three approaches and the reinforcement of the four methods upon each other. It may also depend on jurisdiction, as for example Europe tends to give greater prominence to precaution while the United States assigns a stronger role to liability. In a scenario involving highly uncertain but potentially substantial risks, the balance may shift to give priority to the precautionary principle rather than to risk analysis. However, if strong resilience measures can be put in place, then this would argue for less reliance on the precautionary principle and greater weight to resilience and risk analysis.

Figure 1: Four Principal Tools of Technology Governance (with Examples)

	Permissive	**Prohibitive**
Ex ante	Risk Analysis Example: New Chemical	Precautionary Principle Example: Genetic Modification of Flu Virus
Ex post	Resilience Example: Artificial Intelligence	Liability Example: Autonomous Vehicle Accident

To illustrate, Figure 1 provides an example of where each governance tool may play a predominant role. A new chemical is an

[38] ADAM THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM 1-3 (2014). Thierer defines permissionless innovation as "the notion that experimentation with new technologies and business models should generally be permitted by default. Unless a compelling case can be made that a new invention will bring serious harm to society, innovation should be allowed to continue unabated and problems, if any develop, can be addressed later." *Id.* at 1. By providing a backstop to address any problems that do develop, a resilience-based approach is complementary to permissionless innovation.

example of a technology that can be primarily regulated using risk analysis. The chemical can be tested in various types of *in vitro* and animal assays, and combined with tools like QSAR and exposure analysis, can provide a reasonably accurate estimate of the likely risks of the chemical which can then be managed by traditional risk-based regulatory programs.[39]

An example of an activity that should primarily be governed by the precautionary principle is the genetic modification of viruses, such as the modification of the H5N1 influenza virus to increase its contagiousness or pathogenicity.[40] While such research may be useful for better understanding the risk of and defense to such a modification occurring naturally or by malevolent actors, it carries a high risk of creating an irreversible and catastrophic risk if the modified virus was to escape. Accordingly, such research should only be done under the most precautionary safeguards, if at all.

An example where liability may be the primary approach is autonomous car accidents. Autonomous cars are likely to have a major overall net safety benefit, so this is not a technology we want to impede.[41] Nevertheless, accidents will occur and injuries will result. For the parties involved in the accident, the harm will have been done, and there will be no resilience strategy available (although resilience will still play a role in understanding the accident and modifying autonomous car algorithms to prevent recurrence of such accidents). To both compensate the victims of such accidents and to provide incentives for autonomous car manufacturers to seek optimal safety of their products, liability will be the preferred governance option.

Finally, artificial intelligence is an example of an emerging technology that is best managed with resilience strategies. There are concerns that artificial intelligence will one day gain "superintelligence" and destroy mankind.[42] However, such risks are

[39] Of course, no governance system is perfect, and there will sometimes be surprises from new chemicals that present unanticipated risks. A classic example is chlorofluorocarbons, which presented a risk that was not anticipated by traditional risk analysis. *See* Holger Hoffmann-Riem & Brian Wynne, *In Risk Assessment, One Has to Admit Ignorance*, 416 NATURE 123, 123 (2002).

[40] *Cf.* Seumas Miller & Michael J. Selgelid, *Ethical and Philosophical Consideration of the Dual-Use Dilemma in the Biological Sciences*, 13 SCI. ENG. ETHICS 523, 535 (2007) (implicating the dangers associated with researchers mixing avian flu and human influenza viruses together for purposes of determining public health risks associated with this happening naturally).

[41] *See* Bryant Walker Smith, *Automated Driving and Product Liability*, 2017 MICH. ST. L. REV. 1, 15-17 (2017).

[42] *See* NICK BOSTROM, SUPERINTELLIGENCE: PATHS, DANGERS, STRATEGIES 140-55

diffuse and distant, and do not justify foregoing the major benefits that artificial intelligence can bring. The optimal strategy is likely a resilience approach — of both monitoring for early detection of potential real risks from artificial intelligence and building in resilience measures such as "kill switches" if and when a harmful application does emerge.[43]

II. THE RISE OF RESILIENCE

Resilience, in its most simple form, is the capacity of a system to deal with harm.[44] A resilience approach does not necessarily try to maintain stability or equilibrium. Rather, it recognizes that changes are inevitable in complex systems, and tries to manage and adapt to that change in ways that protect and preserve the core values and functions of the original system. Thus, resilience is "the capacity of a system to experience shocks while retaining essentially the same function, structure, feedbacks, and therefore identity."[45] Resilience has been described as a strategy to ensure a "soft landing" after a significant external shock or disruption causes damage.[46]

As discussed above, resilience is different from, but complementary to, traditional *ex ante* risk assessment and risk management approaches for avoiding or preventing harm, which are well-entrenched in regulatory law.[47] Both risk-based regulation and resilience can be anticipatory, but risk-based approaches try to prevent or minimize the likelihood of harm occurring in the first place, while

(2014).

[43] *See infra* notes 145-46 and accompanying text.

[44] There is significant confusion and ambiguity about the meaning of "resilience." *See* DAVID CHANDLER, RESILIENCE: THE GOVERNANCE OF COMPLEXITY 5 (2014); Dave Hodgson et al., *What Do You Mean, "Resilient"?*, 30 TRENDS ECOLOGY & EVOLUTION 503, 503 (2015). The New York Times recently described resilience as "a word that is somehow so conveniently vacant that it manages to be profound and profoundly hollow." Parul Sehgal, *Brace Yourself*, N.Y. TIMES MAG., Dec. 6, 2015, at 19.

[45] Brian Walker et al., *A Handful of Heuristics and Some Propositions for Understanding Resilience in Social-Ecological Systems*, ECOLOGY & SOC'Y (2006), https://www.ecologyandsociety.org/vol11/iss1/art13/.

[46] Igor Linkov et al., *Resilience: Approaches to Risk Analysis and Governance*, *in* IRGC RESOURCE GUIDE ON RESILIENCE 2 (2016), https://www.irgc.org/wp-content/uploads/2016/04/Linkov-Trump-Fox-Lent-Resilience-Approaches-to-Risk-Analysis-and-Governance-1.pdf.

[47] There is much confusion in the literature about the relationship of risk and resilience approaches. *See id.* ("Some risk managers oppose risk and resilience, some articulate the two concepts for their complementarity, some say that risk is part of resilience, others say that resilience is part of risk.").

resilience strategies seek to minimize the severity or duration of unanticipated harm once an adverse event or outcome has occurred.[48] While risk analysis and resilience are complementary and can work together, traditional risk analysis approaches work best for relatively straightforward and anticipated risks, from a new chemical or drug, for example.[49] In contrast, resilience is best suited for more complex systems that have the potential to create unanticipated or sudden surprises that were not foreseeable or preventable *ex ante*.

An important advantage of resilience-based strategy for governing emerging technologies is, therefore, that "[r]esilience is a property of the entire system and should be assessed accordingly."[50] Emerging technologies are not just machines, products, or instruments in isolation, but rather represent a combination of scientific, technological, economic, political, social, ethical, and legal components that together create a technology scheme.[51] Unlike *ex ante* risk analysis approaches, which attempt to disaggregate such complex technological systems into individual components, resilience is based on the operation of the mechanism as a whole, and thus represents a more holistic and perhaps effective focus of governance.[52]

Resilience can be seen as having two dimensions. The first dimension is the capacity of the system to minimize the extent and severity of harm when something does go wrong. The second dimension is the capacity of the system to recover when harm does occur.[53] For example, consider the response of a local electricity distribution system to a severe storm. The first dimension of resilience is to minimize the number of households that will lose power in that

---

[48] *See* FIKSEL, *supra* note 3; Igor Linkov et al., *Changing the Resilience Paradigm*, 4 NATURE CLIMATE CHANGE 407, 407-09 (2014) [hereinafter Linkov, *Resilience Paradigm*]; Nicole R. Sikula et al., *Risk Management Is Not Enough: A Conceptual Model for Resilience and Adaptation-Based Vulnerability Assessments*, 35 ENVTL. SYSTEMS DECISIONS 219, 220 (2015).

[49] Igor Linkov et al., *Risk and Resilience Lessons from Venice*, 34 ENVTL. SYSTEMS DECISIONS 378, 379 (2014) ("Risk management is [a] useful method for mitigating damage from a known set of threats, but when the possible threat or threat mechanism is unknown or misperceived, risk assessment is impossible and risk management is futile."); Timothy Malloy et al., *Risk-Based and Prevention-Based Governance for Emerging Materials*, 50 ENVTL. SCI. & TECH. 6822, 6822 (2016).

[50] Igor Linkov et al., *Resilience Metrics for Cyber Systems*, 33 ENVTL. SYSTEMS DECISIONS 471, 472 (2013) [hereinafter Linkov, *Resilience Metrics*].

[51] *Id.*

[52] *Id.*

[53] Cameron A. MacKenzie & Christopher W. Zobel, *Allocating Resources to Enhance Resilience, with Application to Superstorm Sandy and an Electric Utility*, 36 RISK ANALYSIS 847, 859 (2016).

storm. The second dimension is how fast the power company can restore power to homes that do lose power.[54]

The importance of resilience has rapidly emerged in the past decade in the context of disaster response.[55] Recent natural disasters such as Hurricane Katrina in 2005 and the Fukushima nuclear plant accident after an earthquake in 2011 have increased the attention and importance given to resilience.[56] Given that natural disasters are inevitable, there is growing recognition of the need to design and implement better strategies to minimize their negative impact and to accelerate recovery, thus pushing resilience to the front line of disaster planning.[57]

The various applications and benefits of resilience go beyond natural disasters. As technologies have become more powerful, complex, and inter-connected, the potential for an unanticipated accident or other unintended consequences also has grown.[58] Examples include the 2003 power outage in Northeast states caused by a single alarm processor failure that snowballed into the loss of power to approximately 50 million people,[59] the Deepwater Horizon oil spill of 2010,[60] and the slow response to the drinking water contamination in Flint, Michigan beginning in 2014.[61] Natural events, human error, or intentional malfeasance can cause technological failures with increasingly severe consequences. This threat to public health, safety, and security has spawned the renewed interest in resilience as a strategy to try to minimize the consequences of technology-related accidents or other adverse effects when they inevitably occur.

---

[54] *See id.*

[55] FIKSEL, *supra* note 3, at 6-15; JUDITH RODIN, THE RESILIENCE DIVIDEND 3-8 (2014).

[56] Jeryang Park et al., *Lessons in Risk- Versus Resilience-Based Design and Management*, 7 INTEGRATED ENVTL. ASSESSMENT & MGMT. 396, 396-97 (2011).

[57] THE NAT'L ACADEMIES, DISASTER RESILIENCE: A NATIONAL IMPERATIVE 1 (2012).

[58] *See generally* CHARLES PERROW, NORMAL ACCIDENTS: LIVING WITH HIGH-RISK TECHNOLOGIES (1999) (noting that the risk of unanticipated accidents increases as technologies grow more complex).

[59] N. AM. ELEC. RELIABILITY COUNCIL, TECHNICAL ANALYSIS OF THE AUGUST 14, 2003, BLACKOUT: WHAT HAPPENED, WHY, AND WHAT DID WE LEARN? 1, 27 (July 13, 2004), http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf.

[60] Park et al., *supra* note 56, at 397.

[61] Kelsey J. Pieper et al., *Flint Water Crisis Caused by Interrupted Corrosion Control: Investigating "Ground Zero" Home*, 51 ENVTL. SCI. & TECH. 2007, 2009-11 (2017) (noting that the Flint water crisis arose due to a complex mix of technologies in which galvanized iron pipes that were originally connected to lead pipes accumulated lead on their iron pipe internal coating and that lead was released when Flint River water was diverted into pipes without corrosion inhibitors).

Resilience is based on the concept that while the optimal strategy is usually to prevent harm from occurring in the first place, often it is not possible or feasible to prevent a harmful event. In that case, the focus must shift to minimizing the extent, duration of, and recovery from the harm. This is analogous to the role of a combination of secondary and tertiary prevention in medicine.[62] While primary prevention's goal is preventing illness or injury prior to its occurrence, secondary prevention's focus is on reducing the effect of illness or injury that has occurred (e.g., screenings, medication). Likewise, tertiary prevention's aim is reducing resulting long-term effects (e.g., rehabilitation and health management programs). Thus, in the medical context secondary prevention reduces the immediate scope and breadth of an injury and tertiary prevention reduces its potential ongoing impacts, encouraging recovery. These types of preventive approaches are applicable to the area of emerging technologies, where systems can never be proven one hundred percent safe and where, inevitably, negative outcomes will occur despite precaution, risk analysis, and liability deterrence. Such incidents may be due to mistake, unexpected events, bad use of technology, and a number of other possibilities. If primary prevention is not possible, then secondary prevention to mitigate the immediate effects and tertiary prevention to try to restore the system's long-term functionality become paramount.

To date, resilience has primarily been implemented as a voluntary or managerial activity by various professions and experts such as engineers, environmental planners, disaster management officials, and product designers. Beyond disaster response, the concept of resilience has expanded to a variety of other scientific and technological contexts such as climate change adaption, environmental management, telecommunications, cybersecurity, and health care readiness. In each context, resilience has generally been applied as a management tool or practical measure, but not as a legally-specified requirement.[63] The law has been slow to integrate resilience strategies, probably because

[62] *Cf.* Barbara Starfield, *Public Health and Primary Care: A Framework for Proposed Linkages*, 86 AM. J. PUB. HEALTH 1365, 1367-68 (1996) (noting that secondary prevention centers on early detection, and tertiary prevention focuses on preventing disease progression or reversal).

[63] *See generally* J. Park et al., *Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems*, 33 RISK ANALYSIS 356 (2013) (regarding resilience as an element of what a system does, rather than simply what the system has); Abdul-Akeem Sadiq & John D. Graham, *Exploring the Predictors of Organizational Preparedness for Natural Disasters*, 36 RISK ANALYSIS 1040 (2016) (discussing resilience in the context of organization leaders and risk managers).

resilience involves a commitment to fluidity and malleability that may be contrary to the traditional legal purpose of ensuring stability and predictability.[64]

Indeed, law has generally been "treated as an inconsequential aspect" of resilience strategies.[65] There has been very little guidance, mandate, or direction from law or regulation on imposing and implementing resilience strategies and systems.[66] As environmental law professor Nicholas Robinson has noted, "[l]aw . . . rarely recognizes or values resilience today as a legal concept."[67] Yet, there are numerous provisions in environmental law and other areas of law that incorporate resilience principles and approaches even without using the term resilience.[68]

A shift to greater reliance on resilience in regulatory law will mean moving from the current static model of regulation that attempts to understand and shape the world *ex ante*, to a more dynamic model that recognizes the need to nimbly shift requirements and approaches in response to real world developments. The current administrative law paradigm encourages a "one and done" front-end rulemaking,[69] which fails to anticipate or accommodate unanticipated consequences or phenomena encountered post-enactment of the governing statute or

[64] *Cf.* Craig R. Allen et al., *Adaptive Management for a Turbulent Future*, 92 J. ENVTL. MGMT. 1339, 1343 (2011) ("The adversarial character of administrative law, combined with the need for certainty (e.g., procedural rules) in the larger realm of American law, is likely incompatible with adaptive management." (citation omitted)); Barbara A. Cosens, et al., *The Role of Law in Adaptive Governance*, 22 ECOLOGY & SOC'Y, no. 1, art. 30, 2017, at 1 (explaining how "legal systems are also purposely structured to prefer the status quo by fostering stability and predictability" and that "[a]s a result of this stabilizing structure, legal systems may pose barriers to adaption").

[65] Olivia Odom Green et al., *Barriers and Bridges to the Integration of Social-Ecological Resilience and Law*, 13 FRONTIERS ECOLOGY & ENV'T 332, 332 (2015).

[66] *See generally* Tracy-Lynn Humby, *Law and Resilience: Mapping the Literature*, 4 SEATTLE J. ENVTL. L. 85 (2014) (tracing resilience deficiencies in law and governance).

[67] Nicholas A. Robinson, *Keynote: Sustaining Society in the Anthropocene Epoch*, 41 DENV. J. INT'L L. & POL'Y 467, 495 (2013).

[68] *See* Gary E. Marchant & Yvonne A. Stevens, *Resilience in Environmental Law: Existing Measures*, 31 NAT. RESOURCES & ENV'T 8, 8-11 (2017).

[69] Robert L. Glicksman & Sidney A. Shapiro, *Improving Regulation Through Incremental Adjustment*, 52 U. KAN. L. REV. 1179, 1179-84 (2004). Ruhl and Fischman use the metaphor of a toggle switch and a dial to explain this distinction. The current legal system operates like a toggle, the regulatory agency finalizes a rule, and then it is turned on and is implemented in that "on" position without any modifications. What is needed for complex systems and technologies is a dial that can be continually adjusted in response to new inputs. J.B. Ruhl & Robert L. Fischman, *Adaptive Management in the Courts*, 95 MINN. L. REV. 424, 438 (2010).

regulation.[70] This is the antithesis of an effective resilience system. As elaborated below, there is a need for a significant shift in the existing paradigm for regulatory law from primarily an *ex ante* approach to a problem to a more progressive legal system providing ongoing, flexible, adaptive, and dynamic vigilance — a form of "learning-by-doing."[71]

Such a shift to promote greater resilience through law would be consistent with more general recent proposals for a more adaptive regulatory system for many emerging technologies.[72] It is also consistent with a 2011 White House Memorandum to federal regulatory agencies on "Principles for Regulation and Oversight of Emerging Technologies," which instructed agencies to "provide sufficient flexibility to accommodate new evidence and learning and to take into account the evolving nature of information related to emerging technologies and their applications."[73] Because traditional administrative law is not conducive to such flexible and adaptive regulatory controls, much of the governance initiatives for emerging technologies such as nanotechnology, synthetic biology and artificial intelligence have involved "soft law" approaches incorporating codes

[70] *See* Green et al., *supra* note 65, at 333; David J. Yu et al., *Aligning Different Schools of Thought on Resilience of Complex Systems and Networks*, *in* IRGC RESOURCE GUIDE ON RESILIENCE 4 (2016), https://www.irgc.org/wp-content/uploads/2016/04/Yu-Rao-Aligning-Different-Schools-of-Thought-on-Resilience-of-Complex-Systems-and-Networks.pdf ("The basic idea is that risk analysis alone is insufficient for dealing with irreducible uncertainties associated with complex systems and thus should be accompanied by improved adaptability [through resilience-based strategies].").

[71] Yu et al., *supra* note 70, at 3 ("[W]hen specificity or predictability of key outputs and system dynamics is high, risk analysis can still be useful and planned adaptation or deliberate transformation can be possible. When the opposite is true, learning-by-doing may be necessary and unplanned adaptation or forced transformation is more likely.").

[72] *See generally* Jennifer Kuzma et al., *An Integrated Approach to Oversight Assessment for Emerging Technologies*, 28 RISK ANALYSIS 1197 (2008) (developing an "integrated oversight assessment" as a tool for evaluating systems that oversee emerging technology); Gary E. Marchant et al., *Risk Management Principles for Nanotechnology*, 2 NANOETHICS 43 (2008) (calling for "[a] more reflexive, incremental, and cooperative risk management approach" to cope with the risks posed by emerging technologies); Gurumurthy Ramachandran et al., *Recommendations for Oversight of Nanobiotechnology: Dynamic Oversight for Complex and Convergent Technology*, 13 J. NANOPARTICLE RES. 1345 (2011) (suggesting overarching inter-agency coordination to meet the challenges created by nanobiotechnology).

[73] Memorandum from John P. Holdren et al. on Principles for Regulation and Oversight of Emerging Technologies 2 (Mar. 11, 2011), http://www.thecre.com/pdf/20110317_Principles-for-Regulation-and-Oversight-of-Emerging-Technologies-new.pdf.

of conduct, private standards, and partnership programs rather than traditional regulation.[74]

Indeed, emerging technologies, for the reasons stated above, represent some of the best opportunities and growing necessity for employing a more resilience-centered regulatory approach. The large uncertainties about risks and benefits make *ex ante* approaches, whether risk-based or precaution-based, particularly prone to error.[75] In most cases, if the technology does present risks, they may only be predictable or detectable after the technology has been deployed, as pre-implementation risks may be unknown.[76] Traditional *ex ante* tools such as risk assessment or life cycle assessment are not viable for complex and highly uncertain systems and discoveries such as nanotechnology or synthetic biology.[77] A resilience-based approach "recognizes uncertainty as an integral component of the decision-making process and reduces uncertainty, not by eliminating variables . . . but by learning from the system through monitoring, feedback, and cycles of adaption."[78] In other words, resilience is based on real-world data rather than speculation.

In addition, while the goal of risk prevention is appealing, the reality is that risk prevention is simply not possible for complex modern technologies: "The increasing complexity, interconnectivity and interdependency of technology make guaranteed protection impossible."[79] Even if we knew all the potential harm scenarios associated with a complex emerging technology (which is not possible), it would nevertheless be too costly and time prohibitive to try to assess the probability and consequences of every scenario.[80]

---

[74] *See, e.g.*, Kenneth W. Abbott et al., *Soft Law Oversight Mechanisms for Nanotechnology*, 52 JURIMETRICS 279 (2012) (evaluating eleven soft law approaches in the United States, European Union, and transnational approaches).

[75] *See* Park et al., *supra* note 56, at 396. In contrast, "less severe and better characterized hazards are better served by existing conventional [risk analysis] methods that adequately assess perceived costs and benefits for a given action." Linkov et al., *supra* note 46, at 10.

[76] FIKSEL, *supra* note 3, at 24.

[77] Thomas P. Seager et al., *Why Life Cycle Assessment Does Not Work for Synthetic Biology*, 51 ENVTL. SCI. & TECH. 5861, 5861-62 (2017).

[78] Green, *supra* note 65, at 334 (citation omitted).

[79] CRO FORUM, CYBER RESILIENCE: THE CYBER RISK CHALLENGE AND THE ROLE OF INSURANCE 3 (Dec. 2014), https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf; *see also* Linkov, *Resilience Metrics*, *supra* note 50, at 471 ("Despite continual progress in managing risks in the cyber domain, it is clear that anticipation and prevention of all possible attacks and malfunctions are not feasible for current or future cyber and infrastructure systems.").

[80] Linkov et al., *Resilience Paradigm*, *supra* note 48, at 407.

Thus, unless society concludes that the hypothetical risks of a new technology justify foregoing the benefits of the technology altogether, justified only in the most extreme cases of serious, irreversible risk, the only path forward will be to proceed with the technology, and monitor it to detect any unanticipated adverse effects as quickly as possible.[81] As Aaron Wildavsky argued, "trial-and-error risk taking, rather than risk aversion, is the preferable strategy for securing safety. Encouraging trial and error promotes resilience — learning from adversity how to do better — while avoiding restrictions that encourage the continuation of existing hazards."[82] Thus, the trial-and-error approach necessitated for most emerging technologies is inherently a resilience-based strategy.[83]

III. PROCEDURAL AND SUBSTANTIVE RESILIENCE APPROACHES

While resilience involves steps and processes that are triggered after a failure or harm occurs, resilience strategies should be built into systems up front to facilitate the quickest and most effective response and adaption when an adverse effect occurs.[84] In other words, we need planned resilience — which does not depend on knowing the exact form or extent of the ensuing harm, which is often unforeseeable.

There are two major categories of potential adaptive legal resilience measures that could be planned in advance and applied to emerging technologies — procedural and substantive.[85] Procedural resilience measures put in place a process for early detection and amelioration of problems or harm. Substantive resilience measures put in place anticipatory harm reduction and adaption preparations or measures to be better prepared to deal with harm if and when it occurs. In this section, we identify some key procedural and substantive resilience governance tools that may be relevant for oversight of emerging technologies, drawing on previous examples and precedents where they exist.

---

[81] THIERER, *supra* note 38, at 37 (supporting "trial-and-error" approach for most risks).

[82] WILDAVSKY, *supra* note 5, at 2.

[83] As discussed above, this is the likely approach we will need to take to govern the risks of artificial intelligence, for example. *See supra* notes 75-78 and accompanying text.

[84] Linkov, *Resilience Paradigm*, *supra* note 48, at 407.

[85] Marchant & Stevens, *supra* note 68, at 8.

A. Procedural Resilience Governance Tools

Procedural resilience is woven into both the secondary and tertiary preventive approaches, discussed above, that may be used in the design of management programs to address potential immediate and longer term adverse impacts from emerging technologies. Many of these procedural resilience tools fall under the term "adaptive management"[86] and are inextricably linked to the latter. The following summary of procedural resilience tools that may apply to emerging technologies begins with a general discussion of adaptive management, and then discusses more specific applications or forms of the general theme of adaptive management.

1. Adaptive Management

Adaptive management is a structured, iterative process of decision-making in the face of uncertainty. Its aim is to reduce concerns and harms over time by system monitoring. It is an especially useful tool when it comes to the adoption of regulations, legislation, and standards pertaining to emerging technologies. This is due to the fact that current technologies and the contexts in which they are applied are constantly evolving, creating consequences that are typically not capable of anticipation when the initial *ex ante* management measures would be adopted. The exponential growth of many different fields of science and technology necessitates more malleable oversight regimens. Areas such as synthetic biology, nanotechnology, 3-D printing, fracking, automated systems, the internet-of-things, and so forth coupled with their safety, security, and financial impact on various industries — such as health, transportation, agriculture, insurance, legal, and manufacturing — cannot evolve within a static regulatory scheme.

Nonetheless, obstacles may initially impede system refinement or complete overhaul toward a more adaptive management oversight process, including impediments such as regulatory precedent, administrative barriers, restrictions on discretion, and uncertainty. For example, the Administrative Procedure Act ("APA"),[87] which federal agencies are subject to, runs counter to adaptive management in its

[86] Adaptive management was first described in the 1970s in the context of natural resource management, in which a cycle of intervention, monitoring, assessment and then policy revisions was implemented to address the inherent uncertainties with natural systems. *See* Charles S. Holling, *Resilience and the Stability of Ecological Systems*, 4 ANN. REV. ECOLOGY SYS. 1, 9 (1973).

[87] 5 U.S.C. §§ 551-559 (2012).

current form. Administrative agencies are required to partake in extensive, procedurally time-consuming activities geared toward public participation and judicial review before setting final rules — a lengthy, time-consuming effort that is not in harmony with the speed of innovation.[88] For example, many major U.S. rulemakings take six to eight years to complete.[89] As such, there is no process in place for leaving things "up in the air" or subject to alteration. Moreover, adjustments or revisions to the initial regulations require an equally lengthy and burdensome procedure, deterring agencies from undertaking such amendments. Learning by doing does not complement the APA.

2. Mandatory Periodic Review Requirements

One way to foster adaptive management is to require a regulatory agency to periodically review its oversight programs. This could be accomplished through laws that integrate procedural resilience such as built-in review and reconsideration requirements that obligate regulators to ensure that any existing regulatory standards are meeting statutory objectives. Some regulatory programs require existing standards to be reviewed on a periodic basis, creating an opening for updating and reconsidering the appropriateness of the existing standards for the problems they are trying to address.[90] Such "[p]lanned windows" provide a "structured and predictable period" to assess a program's success and the possibility of undetected or uncontrolled harm, thus providing stability simultaneously with flexibility to invoke resilience strategies.[91]

---

[88] *See* Gary E. Marchant, *The Growing Gap Between Emerging Technologies and the Law*, *in* THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT: THE PACING PROBLEM 19-33 (Gary E. Merchant et al. eds., 2011) (describing the growing gap between the speed of technological innovation and pace of regulation).

[89] Richard J. Pierce, Jr., *Rulemaking Ossification Is Real: A Response to Testing the Ossification Thesis*, 80 GEO. WASH. L. REV. 1493, 1496 (2012).

[90] *See, e.g.*, 42 U.S.C. § 7409(d)(1) (2012) (requiring Clean Air Act National Ambient Air Quality Standards to be reviewed every five years). Although this program is the classic example of a regulatory program with built-in periodic reviews, the program has many other problems that have impeded its success. *See, e.g.*, Cary Coglianese & Gary E. Marchant, *Shifting Sands: The Limits of Science in Setting Risk Standards*, 152 U. PENN. L. REV. 1255 (2004) (describing how the EPA exaggerated the role of science to evade responsibility for having to give careful reasons for the value judgments embedded in its decisions).

[91] Daniel A. DeCaro et al., *Legal and Institutional Foundations of Adaptive Environmental Governance*, ECOLOGY & SOC'Y (2017),

In addition, there are mandates containing built-in review provisions to oversee the feasibility and resilience of regulatory programs themselves, as opposed to the underlying environmental concern necessitating oversight. This was the case in 1990, when the California Air Resources Board ("CARB") implemented a vigorous program promoting electric vehicles. By 1998, two percent of each large vehicle manufacturer's sales fleet had to be zero emission vehicles, increasing to ten percent by 2003.[92] However, recognizing that this technology-forcing directive may not be sustainable, CARB committed to review the program every two years. This, eventually, resulted in its relaxation, making it more feasible and resilient.

Such mandatory review requirements may provide an effective oversight approach for rapidly emerging technologies. If an agency knows it will be required to revisit or fine-tune its regulatory program every two or five years, it may be less compelled to put in premature regulatory requirements for future applications of the technology, and instead wait until the technology is more mature before taking regulatory action.

3. Sunset Provisions

A related tool would be sunset provisions, in which regulatory programs automatically terminate after a specified period (often five years), and must be affirmatively reauthorized before continuing.[93] Like the mandatory review requirements, sunset provisions force the agency to reconsider its regulatory programs, helping to ensure the measures adjust to rapidly changing technologies. Sunset provisions provide an even stronger weapon against regulatory inertia, because if the agency fails to actively re-enact its regulatory program, the regulatory program ceases to exist by default.

4. Mandatory Adaption Planning

Yet another procedural resilience tool is to require agencies to actively plan to mitigate or adapt to potential adverse outcomes. Climate change adaption is an example where such a procedural resilience tool comes into play. Federal, State, and local initiatives have been actualized to plan for or determine the ability of an affected

https://www.ecologyandsociety.org/vol22/iss1/art32/.

[92] *See* Marchant & Stevens, *supra* note 68, at 9.

[93] *See* Sofia Ranchordás, *Innovation-Friendly Regulation: The Sunset of Regulation, the Sunrise of Innovation*, 55 JURIMETRICS 201, 205-06, 219 (2015).

area to respond and adapt to climate change impacts — thereby also encompassing complementary secondary and tertiary prevention. For example, the EPA has created an assessment tool that evaluates urban communities' resilience to climate change effects. Also, many State and local governments have initiated resilient processes addressing climate change.[94] For instance, the New York Community Risk Reduction and Resiliency Act[95] directs that all state-funded projects consider the potential of climate change consequences during the planning process. While these climate change adaption programs are an example of top-down governmental resilience planning, a manufacturer on its own initiative or as a legal requirement could put in place its own mitigation plan that requires periodic review and revision. For example, a company that manufactures a synthetic biology or artificial product that is commercially released on a broad scale could put into place emergency plans for implementation if its technology escapes control.

5. Post-Market Monitoring

A key aspect of a successful resilience approach is the capability to detect a problem as early as possible in order to minimize the extent of damage caused before the harmful activity and product can be stopped or better controlled. This objective can be achieved by putting in place a post-market monitoring system designed to detect and trigger corrective measures (the substantive response to findings of problems by early detection are discussed in substantive resilience measures below). Effective post-market monitoring can be difficult, expensive, and burdensome.[96] Nonetheless, there has been significant progress in advancing the legal and technological ability to conduct post-market surveillance in recent years, ranging from products such as drugs and

[94] *See State and Local Climate Adaptation*, CTR. FOR CLIMATE & ENERGY SOLUTIONS, https://www.c2es.org/us-states-regions/policy-maps/adaptation (last visited July 31, 2017); *State and Local Adaptation Plans*, GEO. CLIMATE CTR., http://www.georgetownclimate.org/adaptation/plans.html (last visited July 31, 2017).

[95] S. 6617-B, 2013-2014 Leg. Sess. (N.Y. 2014).

[96] *See* THE NAT'L ACADEMIES, GENE DRIVES ON THE HORIZON: ADVANCING SCIENCE, NAVIGATING UNCERTAINTY, AND ALIGNING RESEARCH WITH PUBLIC VALUES 87 (2016) [hereinafter NAS, GENE DRIVES] ("Monitoring and surveillance are necessary to determine whether the approach continues to work over time, but these activities can be expensive and logistically challenging, particularly for low- and middle-income countries. Thus, it will be important to select the measurement tools, timeframes, and protocols that are most informative and sustainable.").

medical devices, to pesticides, to consumer products, to genetically engineered organisms.[97]

6. Adaptive Product Approvals

Adaptive product approval is another procedural resilience measure whereby a product is accelerated onto the market with reduced or minimal regulatory burdens, but then closely monitored for any real world adverse effects which would trigger additional controls. For example, the Food and Drug Administration ("FDA") has adopted a series of expedited approval pathways for drugs to satisfy unmet needs,[98] including its Breakthrough Therapy Designation ("BDT"). BDT is an expedited approval process designed to accelerate the development and review of pharmaceuticals intended to treat a life-threatening or serious condition where initial clinical evidence suggests that the drug in question may promote substantial improvement over accessible therapy — though it is restricted to one or more clinically significant endpoints.[99]

Perhaps, at least within the healthcare industry, the most comprehensive adaptive regulation comes in the form of the 21st Century Cures Act,[100] which came into effect on December 13, 2016. It contains specific provisions for accelerated approval for advanced regenerative therapies based on surrogate endpoints, adaptive trial designs, use of real-world evidence, "approval of a supplemental application, with respect to a qualified indication for a drug,"[101] and expedited development and review of devices, among other examples. These various provisions are intended to expedite the pathway to market for beneficial products, with much of the oversight and control shifted to the post-market context based on real-world data.

---

[97] *See, e.g.*, FDA, STRENGTHENING OUR NATIONAL SYSTEM FOR MEDICAL DEVICE POSTMARKET SURVEILLANCE (2012), https://www.fda.gov/downloads/AboutFDA/CentersOffices/CDRH/CDRHReports/UCM301924.pdf (describing FDA's strategy for strengthening post-market surveillance for medical devices); Robert G. Sharrar & Gretchen S. Dieck, *Monitoring Product Safety in the Postmarketing Environment*, 4 THERAPEUTIC ADVANCES DRUG SAFETY 211, 215-17 (2013) (summarizing recent improvements in post-market drug safety programs).

[98] *See* Erin E. Kepplinger, *FDA's Expedited Approval Mechanisms for New Drug Products*, 34 BIOTECH. L. REP. 15, 28 (2015).

[99] Food and Drug Administration Safety and Innovation Act, Pub. L. No. 112-144, § 902, 126 Stat. 1086 (2012).

[100] Pub. L. No. 114-255, 130 Stat. 1033 (2016).

[101] *Id.* § 3031(a).

The European Union is experimenting with an important adaptive approval system for medical products. From March 2014 through April 2016, the European Medicines Agency ("EMA") conducted a pilot project to examine the application of an adaptive management concept with regard to drugs under development.[102] The "Adaptive Pathways" pilot was based on three principles: (1) approval in stages; (2) use of real-world evidence to complement clinical trial data; and (3) timely participation of stakeholders, including patients, regarding a particular drug's development. The program's application is primarily restricted to ailments with high medical needs, with the aim of improving timely access to life-saving medications prior to final regulatory approval. This approach differs from the FDA's BDT in that the latter relies on the identification of clinically significant endpoints and is based on approval before access. The EMA's Adaptive Pathways project begins with drug administration to a restricted group of patients with a narrow indication that may be based on surrogate endpoints as opposed to clinical. Access to and approval for an expanded set of patients is dependent on the outcome of supplementary clinical trials in conjunction with real-life data. It is worth noting that the approval is considered "initial" as opposed to "conditional." A convertible Conditional Marketing Authorization, for life-threatening conditions, is available through the EMA under the Adaptive Pathways program but it is distinguishable from staggered approval. In 2016, at the completion of the pilot project, the EMA determined that the pilot program demonstrated the value of the Adaptive Pathways project and announced its intention to incorporate this option into the drug approval program for Europe.[103]

Interestingly, while the Adaptive Pathways scheme has seemingly been successful, the majority of proposals received during the pilot project from drug developers were rejected.[104] Those rejected were encouraged to pursue conventional development routes. There is an ongoing debate about the benefits of this adaptive approval program in which entities like the German Institute for Quality and Efficiency in Health Care question adaptive licensing and see "its concerns about adaptive pathways confirmed by the EMA report. This is because evidently neither industry nor EMA has a concept as to how real-world data can be used after drug approval to allow drawing reliable

[102] *See* EUROPEAN MEDS. AGENCY, *Final Report on the Adaptive Pathways Pilot* 1 (2016), http://www.ema.europa.eu/docs/en_GB/document_library/Report/2016/08/WC500211526.pdf.

[103] *See id.* at 22.

[104] *See id.* at 10.

conclusions on benefit and harm."[105] However, their opinion is countered by other experts, such as King College pharmaceutical physician Anthony Fox, who claims such opinions opposing adaptive approvals to be unbalanced, and asks why the critics have not quantified the clinical harm that has occurred as a result of the delayed access to valuable medical products.[106] And when it comes to accelerated access, Elaine Schattner, a well-respected physician and medical commentator, has remarked, "I'm less afraid of bad drugs getting approved than of having bureaucracy block their availability to people who want to try those,"[107] thereby highlighting that it is often much easier to point out a program's potential abstract flaws than it is to stand in the shoes of a patient who has an immediate unmet health need due to inflexible regulations or protocols.

7. Polycentricity

Another important procedural tool for promoting resiliency is polycentricity, in which there are multiple, interacting governance bodies with autonomy to take action in response to a problem or harm.[108] The governance bodies might include federal agencies, state and local governments, industry groups, think tanks, auditors, insurance companies, non-governmental organizations, and various types of public-private partnerships. Having multiple, semi-independent entities involved in governance increases the capability of the governance system to react swiftly and more effectively in imposing resilience measures to minimize the harmful effects from a technology mishap.[109]

---

[105] Inst. for Quality & Efficiency in Health Care, *Adaptive Pathways: EMA Still Leaves Open Questions Unanswered*, SCIENCEDAILY (Aug. 9, 2016), www.sciencedaily.com/releases/2016/08/160809122057.htm. Also, according to Courtney Davis, a Senior Lecturer at King's College London, and others, "[e]vidence for benefits to patients and public health of adaptive pathways is lacking or contradictory." Courtney Davis et al., *"Adaptive Pathways" to Drug Authorisation: Adapting to Industry?*, BMJ, Aug. 16, 2016, at 1.

[106] Anthony W. Fox, *Re: "Adaptive Pathways" to Drug Authorisation: Adapting to Industry?*, BMJ (Aug. 16, 2016), http://www.bmj.com/content/354/bmj.i4437/rr.

[107] Elaine Schattner, *Why Patients Support the 21st Century Cures Act*, FORBES (Nov. 30, 2016, 9:54 AM), https://www.forbes.com/sites/elaineschattner/2016/11/30/why-patients-support-the-21st-century-cures-act/#5020734d4dd3.

[108] Manjana Milkoreit et al., *Resilience Scientists as Change-Makers – Growing the Middle Ground Between Science and Advocacy?*, 53 ENVTL. SCI. & POL'Y 87, 90 (2015).

[109] *See* DeCaro et al., *supra* note 91, at 11 fig.4.

8. Emergency Authority

A final procedural resilience tool is for agencies to have authority to take emergency action if and when a problem or failure is identified. When U.S. federal agencies attempt to use an adaptive management approach to respond to changed circumstances or new problems, their actions are often struck down by courts for failing to comply with the rulemaking provisions of the Administrative Procedure Act.[110] If an agency would have to go through a full regulatory proceeding to adopt new or amended regulations to address the problem, or if it was required to continue to apply existing statutory requirements that turn out to be back-firing, then the harm associated with the problem would be more extended or expanded than necessary, the opposite of resilience. U.S. federal agencies have existing authority to adopt direct final rules or temporary rules in an expedited timeline, but these powers are limited (e.g., if a stakeholder objects, the agency must conduct a full rulemaking).[111] Alternatively, when the existing regulatory approach, especially when mandated by statute, is the problem, an agency should have the discretion to "forbear" implementing the statute if necessary to avoid further harms as a result of newly discovered problems. Recent scholarship has supported such an authority for "administrative forbearance."[112] Regulatory agencies should be given greater flexibility to change course quickly to enable more resilient governance of emerging technologies. This can either be accomplished by loosening the procedural bounds on government regulatory agencies, or by greater reliance on "soft law" measures administered by private and non-governmental entities.[113]

B. Substantive Resilience Governance Tools

There are also a number of substantive provisions that can be adopted into law that would ensure a more robust resilience if adverse effects occur. Some of the key categories of tools are described below.

---

[110] *See* Ruhl & Fischman, *supra* note 69, at 445.

[111] Lyn M. Gaudet & Gary E. Marchant, *Administrative Law Tools for More Adaptive and Responsive Regulation*, *in* THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT 167, 173-79 (Gary E. Merchant et al. eds., 2011).

[112] Daniel T. Deacon, *Administrative Forbearance*, 125 YALE L.J. 1548, 1558 (2016).

[113] *See supra* note 76 and accompanying text.

1. Financial Assurance Mandates

An important pre-requisite to an expeditious and robust response to unexpected harms is to have financial resources easily available and accessible to mitigate continuing harm and to repair the harm that has occurred. Requiring the developers of a technology to contribute to a fund, post a bond, purchase insurance, or to otherwise ensure the rapid availability of adequate resources to mount an effective response can help enhance resilience.[114] Such measures are referred to as financial assurance mandates ("FAMs"), and there are numerous existing examples of such approaches.[115]

For example, the Resource Conservation and Recovery Act requires hazardous waste treatment, storage, and disposal facilities ("TSDFs") to provide financial assurance by setting aside adequate resources for any unanticipated post-closure commitments.[116] These resources must be set aside at the time of the original permitting of the facility, even though the problems being targeted may not occur until many years or even decades after the permit approval. The statute also requires TSDFs to carry appropriate liability insurance as a condition of permit approval.[117] A somewhat different approach is the "Superfund" created by the initial Comprehensive Environmental Response, Compensation, and Liability Act which levied an excise tax imposed on chemical feedstocks and petroleum to fund a Trust Fund used for clean-up of abandoned hazardous waste sites.[118]

Following this model, the developer of a potentially dangerous emerging technology could be required to post a bond, purchase insurance, or otherwise demonstrate financial responsibility to ensure there would be sufficient resources available to mitigate any harm that the technology might cause. Such a requirement would not only compensate injured parties and pay for mitigation if harm occurs, but would also provide a financial incentive for producers of the emerging technology to control risks by internalizing the cost of such harms.[119]

---

[114] James Boyd, *Financial Responsibility for Environmental Obligations: Are Bonding and Assurance Rules Fulfilling Their Promise?*, RESOURCES FOR THE FUTURE 9-11 (Aug. 2001), http://www.rff.org/files/sharepoint/WorkImages/Download/RFF-DP-01-42.pdf.

[115] *See* Zachary C.M. Arnold, *Preventing Industrial Disasters in a Time of Climate Change: A Call for Financial Assurance Mandates*, 41 HARV. ENVTL. L. REV. 243, 268-77 (2017) (reviewing empirical records of FAMs for underground storage tanks, oil production and transport facilities, nuclear power plants, and mine reclamation).

[116] 40 C.F.R. § 264, Subpart H (2017).

[117] 40 C.F.R. § 264.147 (2017).

[118] 26 U.S.C. § 9507 (2012).

[119] *See* Arnold, *supra* note 115, at 264.

Given these advantages and the limits of *ex ante* regulation, financial assurance bonds and mandatory insurance have recently been proposed as a governance approach for hydraulic fracturing.[120] However, such an approach discriminates against the emerging technology, putting a thumb on market choices by effectively putting a tax on the emerging technology that competing technologies do not have to pay. Such an approach also disproportionately disadvantages small entities that do not have the capital reserves to post a bond or purchase sufficient liability insurance. For these reasons, this resilience tool should be reserved for the most dangerous emerging technologies that present a credible risk of serious damage.

2. Back-Up Regulatory Programs

A second type of substantive resilience program is to put in place back-up regulatory programs that would automatically kick-in if a technology that is permitted to be commercialized with minimal or no pre-market approval is subsequently found to cause unacceptable harms. Major environmental statutes such as the Clean Air Act ("CAA") and the Clean Water Act ("CWA") utilize back-up programs for when primary risk-mitigation standards fail.[121] For example, the primary focus of the CAA is to ensure regions achieve health-based national ambient air quality standards ("NAAQS"), but the statute also includes a back-up non-attainment program that imposes more stringent requirements for regions that fail to achieve the NAAQS. The CWA has a similar resilience-based remediation program affecting water bodies that fail to comply with applicable water quality standards, triggering a requirement to set and enforce a total maximum daily load for such "impaired" waters.[122]

The Endangered Species Act ("ESA") is another environmental statute where more stringent resilience-themed corrective measures kick in once harm has occurred and a species has been listed as endangered or threatened.[123] For example, the ESA prohibits any person from "taking" an endangered species, either directly by killing or harming members of the endangered species, or indirectly by altering critical habitat in a way that would harm the species.[124]

[120] Dana & Wiseman, *supra* note 31, at 1561-71.

[121] *See* 42 U.S.C. §§ 7501-7515 (2012) (establishing additional regulatory provisions applicable to various air quality "nonattainment areas").

[122] 33 U.S.C. § 1313(d) (2012).

[123] 16 U.S.C. § 1533(d) (2012).

[124] 16 U.S.C. § 1538 (2012).

Similarly, when activities harm wetlands, the CWA requires "compensatory mitigation" to offset and replace the loss of wetlands and restore aquatic resource functions in the watershed.[125]

Some voluntary risk management programs adopt a similar approach by providing an "off ramp" that imposes more formal and stringent regulatory requirements if the voluntary program fails to achieve its stated goals. For example, the National Low Emission Vehicle program,[126] a voluntary program among vehicle manufacturers, states, and the EPA, provides for greater emissions reductions than required by the statute while ensuring that manufacturers are not subject to inconsistent state standards, though nonetheless imposes such an off-ramp for either manufacturers or states if certain assumed conditions are not met or followed.[127] A number of empirical analyses of voluntary regulatory programs has found that the presence of a "regulatory stick" that would be implemented if the voluntary program did not achieve its intended results was a key factor in the success of such voluntary programs.[128]

Of course, it is not usually possible to anticipate how and why a particular technology may cause problems in the future, complicating then the design of back-up regulatory programs that would kick-in if and when such problems occur. While this is a limitation of this particular resilience strategy, the basic idea is that technologies can be given more regulatory freedom to operate without restrictions for as long as they are safe and effective in the marketplace, but if problems occur, a regulatory back-up would be in place to impose more traditional risk-based controls. Thus, employing such an approach, emerging technologies could be allowed to be commercialized with minimal *ex ante* controls, but back-up regulatory systems or "sticks"

---

[125] *See* 33 U.S.C. § 1344 (2012). Compensatory mitigation "refers to the restoration, establishment, enhancement, or in certain circumstances preservation of wetlands, streams or other aquatic resources for the purpose of offsetting unavoidable adverse impacts." EPA, WETLANDS COMPENSATORY MITIGATION 1, https://www.epa.gov/sites/production/files/2015-08/documents/compensatory_mitigation_factsheet.pdf.

[126] Control of Air Pollution from New Motor Vehicles and New Motor Vehicle Engines: State Commitments to National Low-Emission Vehicle Program, 63 Fed. Reg. 926, 926 (1998).

[127] *See id.* at 939-52.

[128] *See, e.g.*, DANIEL J. FIORINO, VOLUNTARY INITIATIVES, REGULATION, AND NANOTECHNOLOGY OVERSIGHT: CHARTING A PATH 25 (Woodrow Wilson International Center for Scholars 2010), http://nanotechproject.org/process/assets/files/8347/pen-19.pdf; David E. Grimeaud, *Convergence or Divergence in the Use of "Negotiated Environmental Agreements" in European and U.S. Environmental Policy: An Overview*, *in* GREEN GIANTS? ENVIRONMENTAL POLICIES OF THE UNITED STATES AND THE EUROPEAN UNION 159, 159-81 (Norman J. Vig & Michael G. Faure eds., 2004).

would be in place that would automatically kick in if the technology is found to cause unanticipated harms.

3. Post-Approval Recall

A related resilience measure is to recall or stop distribution of approved products that turn out to impose significant harms that were not anticipated at the time of approval. If post-approval monitoring (a procedural resilience measure discussed above) detects a significant problem, a regulatory agency empowered with the authority to recall the product could take action to prevent any further injury, thus mitigating the extent of the harm.

The FDA provides an exemplar of the importance of post-approval recall. Under its original authority regulating medical products such as drugs and medical devices, the FDA had strong pre-market approval authority but weak post-market authority. The agency usually had to rely on publicly identifying dangerous products in the hope of encouraging manufacturers to voluntarily withdraw such products. But through a series of statutory amendments that gave the agency more mandatory post-market powers, the FDA has used post-market regulation as a more important and effective part of its risk management strategy.

Granting regulatory bodies stronger post-market authority to restrict or recall products that turn out to be unacceptably dangerous is a resilience strategy, because it reduces the scope of harm once an injury has occurred. Relying on post-market action for agencies that already have such authority, and giving such powers to agencies currently lacking effective post-market controls,[129] would help shift the governance of emerging technologies from *ex ante* to *ex post*, and allow regulatory restrictions to be based on real-world assessments of harm rather than highly uncertain pre-market risk assessments or precautionary restrictions.

[129] For example, the United States Department of Agriculture ("USDA") regulates the agricultural testing and commercialization of genetically modified ("GM") crops. However, once the USDA has approved the commercialization of a GM crop it loses any further regulatory authority over that crop, and has no legal authority to take action if that crop turns out to cause problems. *See* 7 C.F.R. § 340.6(e)(1). This lack of post-market authority likely forces the agency to be unduly precautionary in the pre-market approval, since it knows it has no recourse if it approves a product that turns out to create problems.

4. Redundant Systems

Redundancy is a core resilience measure. It recognizes that safety systems can fail, but the consequences of such failures can be minimized by having a redundant back-up system in place.[130] For example, the nuclear power industry is well-known for establishing redundant systems as part of its fault tree analysis, a systematic analysis of everything that could go wrong, with redundant safety measures built into the system to compensate for any failures. Of course such systems are not perfect, as demonstrated by Chernobyl, Fukushima Daiichi, and Three Mile Island, but even then, redundant safety measures resulted in less harmful events than would otherwise have occurred, and no doubt prevented numerous other failures from escalating into harmful accidents.

Redundant safety measures could be built into emerging technologies to minimize the extent of damage even if some safety measures fail. For example, in deploying gene drives into the wild, several different and redundant or complementary safety systems could be built into the engineered organism to minimize the risk of an adverse effect.[131] Even if one of the safety systems fail, the other redundant systems may still help to mitigate harm.[132]

Of course, redundant systems impose a cost upon the technology developer, which if over-prescribed, can be prohibitive for the technology. Absolute safety and zero risk are not realistic objectives. Thus, redundant safety measures should be considered as part of an overall resilience strategy when such measures are effective, cost-effective, and necessary.

---

[130] *See* Azad Madni & Scott Jackson, *Towards a Conceptual Framework for Resilience Engineering*, 3 IEEE SYS. J. 181, 189 (2009) (explaining how this important safety measure may be accomplished via functional redundancy, which refers to alternative ways to perform the same function that do not rely on the same physical systems, and physical redundancy, which refers to redundant equipment in the same system to protect against equipment failure).

[131] Omar S. Akbari et al., *Safeguarding Gene Drive Experiments in the Laboratory*, 349 SCIENCE 927, 927 (2015) ("Although we differ in our assessments of the types of precaution needed, we recognize that any single confinement strategy could fail. We therefore unanimously recommend that future studies use a combination of stringent confinement strategies . . . whenever possible and always use safeguards adequate for preventing the unintentional release of synthetic gene drive systems into natural populations.").

[132] *See* NAS, GENE DRIVES, *supra* note 96, at 97-99 (recommending several different safeguards that should be used in a complementary manner).

5. Stockpiling

Yet another substantive resilience measure is to stockpile needed mitigation resources and supplies for when something does go wrong. A prominent example of this strategy is the Centers for Disease Control and Prevention's ("CDC's") Strategic National Stockpile, which stores and supplies appropriate "pharmaceuticals and medical supplies for use in a public health emergency severe enough to cause local supplies to run out."[133] As described by CDC:

> The stockpile ensures the right medicines and supplies are available when and where needed to save lives. When state, local, tribal, and territorial responders request federal assistance to support their response efforts, the stockpile ensures that medicine and supplies get to those who need them most during an emergency. Organized for scalable response to a variety of public health threats, the repository contains enough supplies to respond to multiple large-scale emergencies, simultaneously.[134]

A related project is Project Bioshield, a national program not only to stockpile but also to develop vaccines, treatments, and diagnostic devices needed to respond quickly to a bioterrorist attack.[135] This stockpiling strategy is a resilience tool since it provides supplies and resources that can help minimize the harm when a harmful event occurs. It can ensure a more rapid and effective response that can minimize the extent of harm. The delayed responses to recent tragedies such as the Deepwater Horizon, Fukushima, and Flint water disasters significantly expanded the harm from such incidents. If there are known counter-measures that can help mitigate potential adverse effects of an emerging technology, prophylactic production and storage of such products can help ensure any adverse event is more tightly contained. For example, a resilience strategy for a nuclear plant would be to have available robots capable of going into high-radiation areas that humans could not safely enter, but the Japanese nuclear industry apparently failed to develop and stockpile such robots

---

[133] *Strategic National Stockpile*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/phpr/stockpile (last visited July 27, 2017).

[134] *Id.*

[135] *See* Philip Russell, *Project BioShield: What It Is, Why It Is Needed, and Its Accomplishments So Far*, 45 (Supp. 1) CLINICAL INFECTIOUS DISEASES S68, S68-72 (2007).

because of a concern that having such robots would give the public the perception that a safety failure was possible.[136]

6. Kill Switches

A final substantive resilience tool is the designed capability to recall or inactivate a technology or product that is found to be causing unanticipated harms. The original National Institutes of Health recombinant DNA ("rDNA") guidelines encouraged scientists to use biological containment measures that would limit the harm of any modified organisms that were inadvertently released into the environment. For example, many early rDNA experiments used a severely disabled strain of *E. Coli* that was incapable of surviving outside of the laboratory environment.

Some research has been conducted on developing "suicide genes" in genetically modified bacterial or fungi which might be intended for environmental release (e.g., bioremediation).[137] The concept is that an engineered organism would contain a "suicide gene" that would kill the organism if it escaped from a contained site or if it persisted in the environment beyond its intended use.[138] While some progress has been made in developing such systems,[139] they have yet to be demonstrated to be effective in real-world environments.[140] However, the National Academy of Sciences has advocated further research to develop and test such systems.[141]

Similarly, the Presidential Commission for the Study of Bioethical Issues recommended in 2010 the pursuit of "suicide genes" or "kill switches" as a possible mechanism to limit damages caused by synthetic biology organisms that are released or escape into the wild.[142] More recently, proposals to use synthetic biology or gene

[136] J. Park et al., *Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems*, 33 RISK ANALYSIS 356, 361 (2013).

[137] *See* NAT'L RESEARCH COUNCIL, BIOLOGICAL CONFINEMENT OF GENETICALLY ENGINEERED ORGANISMS 173-75 (2004); *see also* S. Molin et al., *Suicidal Genetic Elements and Their Use in Biological Containment of Bacteria*, 47 ANN. REV. MICROBIOLOGY 139, 139-66 (1993).

[138] *See* NAT'L RESEARCH COUNCIL, *supra* note 137, at 173.

[139] *See, e.g.*, Clement T.Y. Chan et al., *'Deadman' and 'Passcode' Microbial Kill Switches for Bacterial Containment*, 12 NATURE CHEMICAL BIOLOGY 82, 85 (2015) (discussing advancements in the biocontainment of genetically modified microbes).

[140] *See* NAT'L RESEARCH COUNCIL, *supra* note 137, at 175.

[141] *See id.* at 195-97.

[142] PRESIDENTIAL COMM'N FOR THE STUDY OF BIOETHICAL ISSUES, NEW DIRECTIONS: THE ETHICS OF SYNTHETIC BIOLOGY AND EMERGING TECHNOLOGIES 70 (2010), http://bioethics.gov/sites/default/files/PCSBI-Synthetic-Biology-Report-12.16.10_0.pdf.

drives to wipe out invasive or pathogen-carrying species such as the *Aedes aegypti* mosquito that carries the Zika virus and other pathogens have included suggestions to include "suicide genes" or "reverse drives" that would essentially allow the engineered species to be recalled if they caused unanticipated ecological or health problems.[143]

Robotic and artificial intelligent systems can also be designed with kill switches that can be used to terminate programs that have escaped control mechanisms.[144] The European Parliament recently passed a resolution that calls on robot designers to include a kill switch in such systems that can be used to deactivate the robot if it is causing problems.[145] Of course, a super-intelligent autonomous system may resist orders or attempts to turn it off by activating a kill switch, but research is providing key insights that building uncertainty into autonomous system utility functions can make such a system less inclined to disable its kill switch.[146] This is the type of anticipatory planning for resilience in the event that something goes wrong that is needed to build safer systems.

CONCLUSION

The current controversy over risk management of emerging technologies is stalemated between traditional risk analysis and the precautionary principle. Both approaches try to prevent risks using *ex ante* approaches, and both are particularly inept for emerging technologies, mainly because of the large uncertainties about speculative future risks and the risk of unduly retarding beneficial new technologies. Resilience offers a new approach for realizing the benefits of emerging technologies while also minimizing their risks. Instead of trying to anticipate such risks before the technologies are commercialized, a difficult if not impossible task, resilience involves a mix of procedural and substantive measures that can be used to

143 *See* Akbari et al., *supra* note 131, at 927.

144 *See* LAURENT ORSEAU & STUART ARMSTRONG, SAFELY INTERRUPTIBLE AGENTS 9-10 (2016), https://intelligence.org/files/Interruptibility.pdf.

145 Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics, EUR. PARL. DOC. (2015/2103(INL)) (2017) (requiring robotic designers to "integrate obvious opt-out mechanisms (kill switches) that should be consistent with reasonable design objectives").

146 *See generally* Dylan Hadfield-Menell et al., *The Off-Switch Game*, ARXIV (June 16, 2017), https://arxiv.org/pdf/1611.08219.pdf (discussing how programming a certain degree of uncertainty about objectives can serve as a kill switch that safeguards against machine-systems developing subgoals that might seek to prevent a human from shutting them off).

quickly detect and minimize harms if and when they occur. By focusing on real world risks when they manifest, rather than speculative risks before the technology exists, resilience promotes more effective risk governance while also allowing technologies relatively unimpeded access to the marketplace.

This paper presents the case for a resilience-based approach to the governance of emerging technologies and offers a toolbox of procedural and substantive resilience measures. Governments charged with oversight of emerging technologies, companies, and other stakeholders seeking to promote responsible development of emerging technologies where government regulations have not yet been formulated, should consider such resilience approaches and tools as part of a holistic governance framework that includes risk analysis, precaution, liability, and resilience. If effective resilience methods are available for a particular technology, they will reduce the reliance on risk analysis, precaution, and liability, and perhaps minimize the detrimental effects of over-relying on such approaches.