The Fortress Problem

Jack Sheldon Anderson

Abstract

Fortresses do not usually fail well. When they rely on robustness or complication, positions of strength are only tolerant of stress up to a defined point or of a certain character. For a fortification that fails to adapt, centralization—even of strength—presents a surprising liability. Fortresses concentrate risk. This paper considers the way in which uncertain and unthinkable events undermine security practices that presume a greater degree of knowledge, uniformity, and control than is available.

When facing worst cases and ambiguous threats, current security doctrine, theory, and practice promise more than they can deliver. Threat and catastrophe highlight a mismatch between reality and approach. Threat may be defined as official danger—governmental certification of possibility. Catastrophe implies rupture and exhaustion of capacity. Two problematic tendencies dominate the security response to threat and catastrophe: applying risk management when the information necessary to support such calculation is not available, and boundless precaution. In the first case the homeland security enterprise lives with a false assumption that it controls the risk; in the second it has little measure of success and surrenders decisions to threat politics. This paper suggests that security agencies need to renovate their fortresses, favoring adaptability over robustness in the face of threat and catastrophe.

The Fortress Problem

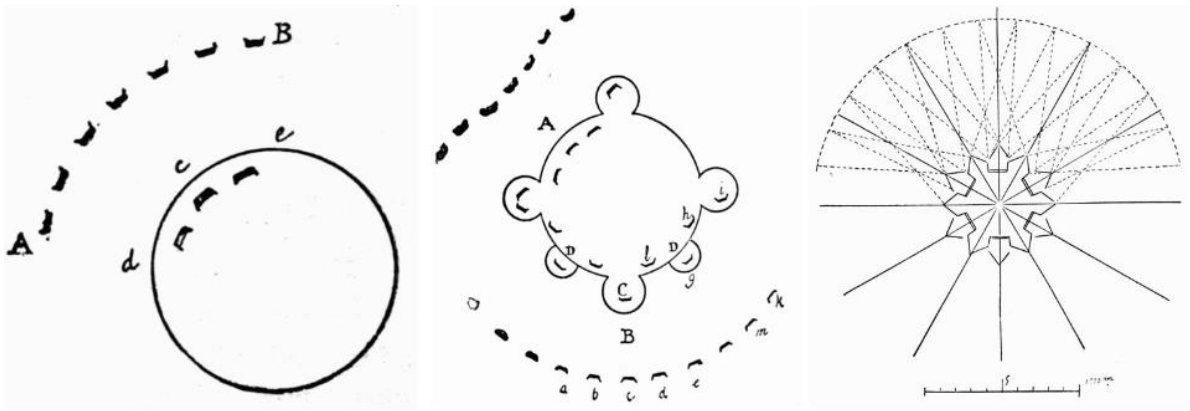
Staircases in medieval castles often spiraled upward clockwise around a central newel. The reasoning for this design tendency, so the theory goes, was to give the advantage to the (right-handed) defender, who had more room to swing his sword from above.[1] There is elegance to this idea. Fortifications may be complicated, but the principle of fortification is simple: attackers and defenders, the forces of good arrayed against the forces of evil, civilization versus barbarism and the outer dark. It is a simplicity that homeland security agencies might envy.

The crash of Germanwings 9525 in March 2015 illustrates a more uneasy insecurity. When the captain left the cockpit during that flight, the co-pilot locked the cabin door and intentionally crashed the aircraft into a mountainside in the French Alps, killing the 144 passengers and 6 crewmembers.[2] For security agencies, the Germanwings crash poses a troubling dilemma. The pilot was able to create astonishing tragedy, not *despite* complicated fortification, but *because* of it.

After the attacks of September 2001 (9/11), security measures in the cockpits of passenger airplanes were designed—like medieval castles—to provide decision and tactical advantage to the defender within the cockpit.[3] The same security measures allowed a co-pilot to prevent a pilot from re-entering the cockpit. Shortly after the Germanwings crash, the European Aviation Safety Agency issued emergency guidance recommending two crew members be in the cockpit at all times.[4] In hindsight, the subsequent review of safety protocols belies a darker concern: procedures must consider more fully how to protect *against* the pilot. The professional most directly responsible for the safety of the plane must be thought of as a liability. "The irony of risk here," says Ulrich Beck, "is that rationality,that is, the experience of the past, encourages anticipation of the wrong kind of risk, the one we believe we can calculate and control, whereas the disaster arises from what we do not know and cannot calculate."[5]

Fortifications must adapt to the threats they face. Writing in the late 19th century, French architect and engineer Eugène-

Emmanuel Viollet-le-Duc provided a primer in fortification. His book *Annals of a Fortress* describes the necessary adaptations that follow advances in technology and evolutions in threat.[6] In its simplest abstract form, a circular enclosure presents a defensive problem: the defender of a fortress is at a disadvantage. Facing an attacker with projectile arms, "the defenders will be able to oppose only an inferior number of engines to the convergent fire."[7] To correct this weakness, variations in defensive measures (including bastions and star-shaped citadels) allow the defender to oppose greater numbers of attackers. The attacker in turn adapts by developing longer distance siege weapons. As this cycle of adaptation continues, the fortress evolves from simple to complicated as technology and tactics alter the paradigm of defense. A principle emerges: protection requires both strength and adaptability.



With this series of figures, Viollet-Le-Duc demonstrates the way that the application of the principles of fortification leads to progressively more complicated defenses. Translated by Benjamin Bucknall, *Annals of a Fortress* (Boston, J. R. Osgood and Company, 1876), Figures 77, 78, and 79.

Figure 1. From Eugène-Emmanuel Viollet-le-Duc, *Annals of a Fortress*.

The Germanwings crash was a deadly reminder that cockpit security protocols must adapt to what seems to be an impossible threat. Hardened fortresses that dominate much security thinking are often revealed as insufficient in dramatic ways, as they were in the case of Germanwings 9525. Risk-based screening employed by the Transportation Security Administration (TSA) separates travelers into groups of higher and lower risk and adjusts screening levels accordingly.[8] In response, an adaptable enemy will simply hide in low risk groups. This possibility was realized recently, as two men were arrested in a gun smuggling operation that relied on one of them having a security clearance and airport access.[9] Even more recently, TSA discovered that 73 airport employees were on terrorist watch lists.[10]

The Paris terror attacks that claimed the lives of more than 100 in November 2015 occurred during a period of heightened awareness and elevated security posture.[11] Perhaps more troubling, the tactics and target selection were generally, if not specifically, anticipated—prefigured by the grisly Mumbai attacks of 2008, and making real the concerns of security agencies. Part of the challenge of this devastating attack is the recognition that it was not a strategic surprise. If the irony of risk is that it encourages the anticipation of known and calculable problems, a second irony of threat and catastrophe is that even known threats are not entirely predictable.[12]

Domestic security agencies have not resolved the competing requirements of what is likely versus what is imaginable. Prevailing theory and approach do not bridge the gap between

the theoretically calculable and the theoretically incalculable, between the probable and the possible. Security agencies, however, live at precisely these crossroads. Worst cases and ambiguous threats are central, not marginal concerns for domestic security. As a result, making rational decisions about profound uncertainties is a crucial responsibility for security agencies.

The 4th century Chinese philosopher Zhuangzi tells the story of Zhuping man, who spent all his wealth and several years mastering the art of slaying dragons, only to find himself in a world without dragons.[13] This is the fortress problem. Security agencies are given impossible responsibility for unthinkable perils, but may not simply decline them, or announce that they are unable to deal with terrorism or catastrophe. Instead, two approaches dominate security decisions about uncertainty: risk assessment, and the precautionary principle. Both prove to be insufficient guides.

Unbounded Risk

In order to understand the probability and consequence of a risk, the analysis of that risk must establish an area of study and an area of impact. Threat and catastrophe, however, have a knack for acquainting security organizations with previously unforeseen or immeasurable dimensions. What is not known becomes the central figure in risk decision-making, not what is known.[14] Modern risks obscure the very dimensions which homeland security organizations are positioned to measure.

As early as 2005, US Department of Homeland Security (DHS) Secretary Michael Chertoff insisted that, "DHS must base its work on priorities driven by risk."[15] Not surprisingly, the DHS annual Financial Report to its oversight and appropriation bodies in Congress for fiscal year 2014 contains more than one hundred references to risk, its management and reduction, and the development of risk-based security measures.[16]

Risk is the preferred tool for making decisions in uncertainty because it supposes calculated rationality. Risk is defined as "the probability and magnitude of a loss, disaster or other undesirable event," or "when it is possible, at least in principle, to estimate the likelihood that an event (or set of events) will occur."[17] In his book *The Taming of Chance*, Ian Hacking has described the invention of risk as a shift out of the world of pure causality. "Causality," says Hacking, "long the bastion of metaphysics, was toppled, or at least tilted: the past does not determine exactly what happens next."[18] Probabilistic thinking changed the relationship humans had with the future, allowing projections of the future to govern the present. Understanding that the future was uncertain—thus unwritten—society had the right to expect greater control over it. Only knowledge sufficient to calculate was wanting.

Risk is synonymous with sobriety: an idea in opposition to politics, fear, and mindless security musculature. For homeland security agencies tasked with responsibly adjudicating the allocation of limited resources to provide protection against an expanding menu of threats and hazards, however, unbounded risk—danger that cannot be fully calculated—is problematic. U.S. counterterrorism officials, reacting to a mass shooting in San Bernardino in December of 2015, expressed their concern that the complexity of factors associated with the attack, including Islamic extremism, possible workplace grievance and legally purchased firearms "exposed a threat matrix that may strain domestic security agencies' capabilities, no matter how aggressively they seek to adapt."[19] It was the deadliest terror attack in the U.S. since 9/11, and came seven days after President Obama assured the nation that there was "no specific and credible intelligence indicating a plot on the homeland."[20] Homeland security includes the incredible.

If security agencies cannot fully calculate how likely something is, or predict specific occurrences, they are equally challenged by measuring how bad an event might be. Contemplating the possible destruction of Earth due to a theoretical particle accelerator accident, Cambridge physicist Adrian Kent notes drily that in addition to the loss of all life on the planet "there is the opportunity costs arising from the absence of future generations."[21] This is a cost beyond accounting.

The difficulties of calculating catastrophe are not limited to such exotic risks. It is not yet possible to calculate the full cost of Hurricane Katrina. As recently as September of 2014, The Federal Emergency Management Agency (FEMA) and the State of Louisiana still retained $812 million in unexpended hazard mitigation grant program funds, nearly a decade after Hurricane Katrina.[22]

Domestic security organizations must be able to make rational decisions even, and particularly, in situations where they lack sufficient information to calculate the likelihood or consequence of a possible event. Security vulnerabilities are highly concentrated, causes are highly distributed, and impacts difficult to measure. In *Worst Cases*, Lee Clarke argues that, "probabilistic thinking is not the only way to be reasonable," suggesting that security agencies need to actively engage possibilities along with probabilities.[23]

For managing very bad, highly uncertain, or complex possibilities, risk has distinct limitations: security agencies still have to manage threat and catastrophe beyond what makes actuarial sense. In situations without sufficient information to estimate risk, security agencies often turn to precaution.

Unrestrained Precaution

When an airplane carrying 224 passengers crashed over the Sinai in October 2015, Lufthansa and Air France, two of the largest airlines in Europe, ceased flights in the region "as a precaution." They did so explicitly "because the reasons for the crash were not clear."[24]

The precautionary principle is often expressed as an idiom: better safe than sorry.[25] The principle "counsels that we should avoid steps that will create a risk of harm; until safety is established through clear evidence, we should be cautious."[26] In a more detailed sense the precautionary principle proposes that, "in the absence of scientific near-certainty about the safety of the action, the burden of proof about absence of harm falls on those proposing the action."[27] Precaution can also reflect a bias for action, particularly when homeland security organizations take precautionary measures against threats and hazards that are uncertain. In this form of precaution, the burden of proof is on those opposing an action to demonstrate that it does not reduce a threat.

On its surface, the precautionary principle appears to be rational, but it is not an effective guide for deciding between uncertainties. Taken seriously, says Cass Sunstein, the precautionary principle would in fact be a "paralyzing principle"—prohibiting any action, since any action designed to address one risk would bring with it potential risks and uncertainties to be cautious about.[28] Action-biased precaution is, conversely, a *permissive* principle—authorizing any action on the basis that it might reduce risk. Applied earnestly, the precautionary principle either prohibits every action, or justifies any action. In either case, precaution is incoherent as a means of guiding decisions, but serves only as the veneer of political advocacy for one action or regulation over another.

Precautionary management of uncertain risks like terrorism becomes less about confronting specific threats that currently exist, and increasingly about the anticipation and prevention of an infinite array of possible futures. In this case, as Aradau and Van Munster argue, "the rationality of catastrophic risk translates into policies that actively seek to prevent situations from becoming catastrophic at some indefinite point in the future."[29] The ongoing debate about the government's ability to collect the phone data of American citizens that it does not currently need—but might eventually need to support intelligence analysis and counterterrorism—is over formalized government precaution.[30] The deadly Paris terrorist attacks in 2015 prompted a precautionary bill in Congress aimed at pausing the admittance of Syrian refugees, not based on information about risk but lack of information.[31] "This is a moment," wrote Representative Paul Ryan, "when it's better to be safe than sorry."[32]

It is difficult to say how much safer precautionary spending and effort makes America. Close to $3.7 billion of TSA's $7.3 billion budget goes to screening.[33] In 2015 TSA screened 708 million passengers and found 2,653 firearms.[34] That is, approximately

0.0004% of passengers had guns confiscated (assuming one gun per incident) and none of them were terrorists. John Mueller contends that in order to break even on counterterrorism spending, from a cost/benefit standpoint the United States would need to be experiencing attacks on the scale of 9/11 at least once a year, or 18 Oklahoma City bombings every year.[35] Meanwhile, the attacks of 9/11 resulted in around $44 billion in insured losses, with direct economic losses estimated at $200 billion.[36] Faced with such catastrophic possibility but uncertain probabilities, it is tough to say to what degree TSA's $3.7 billion screening budget is risk based or precautionary. The safety benefit of interdicting prohibited items in 0.0004% of passengers is also difficult to assess. The same year, the DHS Inspector General found a failure rate for catching prohibited items so high that it "greatly disturbed" the acting TSA chief, which potentially means that significantly higher numbers of firearms flew without incident.[37] TSA's precautionary spending on screening has not interrupted any attempted terrorist attacks, but it is hard to say whether it deterred any.

The motivation behind precaution is noble; an approach intended to oppose undesirable possibilities, without delaying unnecessarily. But precaution is not applied as an equal principle resulting in general caution about everything. Rather, it has encouraged the growth of *threat politics* and a "selectivity of fear."[38] This means fearing, and being cautious about only those threats that are prominent or available. Such availability is subject to the influence of media coverage, parochial concerns, dread of the unfamiliar etc. Precaution then puts risks in the hands of political will, not calculation. Given that homeland security risks are particularly uncertain, domestic security agencies require something better by way of principle.

There is, however, no disputing the success of precaution, or the failure of insufficient caution. After witnessing the ravages of a tsunami in 1933, Kotaku Wamura, the late mayor of the Japanese town of Fudai-Mura, proposed and successfully championed the construction of a $20 million floodwall designed to withstand an improbable 10,000-year recurrence interval tsunami.[39] The effort was widely reviled, but spared the town from destruction in the wake of the massive (and improbable) 2011 tsunami. Conversely, citizens of Flint Michigan might reasonably expect greater precaution from their government with regard to drinking water risks. Likewise, with high uncertainty risks like terrorism or climate change, a certain form of precaution might be necessary to address the insufficiencies of risk.

A disciplined and potentially useful form of precaution may be found in John Rawls' "maximin principle", which contends that in conditions of uncertainty, we ought to rank alternatives by their worst possible outcomes, and pursue the outcome with the best worst case.[40] Refining the thinking of Rawls, Sunstein proposes an "anti-catastrophe principle" as an antidote to the paralysis or spasm of precaution.[41] More disciplined than precaution, anti-catastrophe analysis engages both imagination and calculation. It provides for security agencies a limiting principle to action, preventing excessive commitment, avoiding inaction or handwringing, but permitting action against worst case scenarios.

Unfortunately, the plans and doctrines that security agencies make for impossible tasks are neither fully risk-based nor explicitly precautionary. Risk and precaution both presuppose that in one way or another, through calculation or carefulness, security agencies can account for every eventuality. In this spirit, *The 9/11 Commission Report* admonished the Federal government's supposedly insufficient imagination.[42] According to *The 9/11 Commission Report*, the intelligence, law enforcement, and domestic security and preparedness apparatus of the nation failed to credibly imagine the possibility of an aircraft used as a weapon. The answer to this problem, however, is not to give equal standing to every imagined possibility, or to suppose we are able to imagine every possibility. Such regimes of prediction and control are brittle fortresses. "It is difficult," says Michael Barkun, "to create contingency plans for inconceivable contingencies."[43]

In July 2015, Lloyds of London and the Centre for Risk Studies at Cambridge University

published a scenario analysis of a cyber attack on the US power grid. The results of their study were grim.[44] An attack of relatively limited scope (impacting 50 out of 700 generators across the Northeastern region of the US) triggers a scenario where 93 million people are without power and the impact on the US economy is up to a trillion dollars in the most extreme scenario. Armed with such information, security agencies are tempted to choose between competing apocalypses. Of the fifteen National Planning Scenarios designed in 2005 to support the implementation of Homeland Security Presidential Directive 8 (HSPD-8), twelve were terrorism related. They included blister agent chemical attacks and improvised nuclear devices, but excluded the threat of electromagnetic pulse weapons.[45] In 2014, H.R 3410 set about to correct this oversight. The draft Critical Infrastructure Protection Act or CIPA, which passed the House in 2014, would, "require the Assistant Secretary of the National Protection and Programs Directorate to: (1) include in national planning scenarios the threat of electromagnetic pulse (EMP) events."[46] As a form of precaution, this impulse to add additional scenarios to the menu of security agencies lacks any clear limiting principle. There is little to suggest what threshold of probability or consequence warrants new legislation or a mandated scenario. Further, since it is not possible to account for every eventuality, particularly dreadful or novel risks attract constituencies and political influence to raise their prominence.

The unsuitability of risk management and precaution to unbounded risks has an unfortunate byproduct. The plans and schemes of management that security agencies produce reflect the liabilities of a hyperextended imagination: believing they have accounted for every eventuality, and proposing excessively detailed scripts for managing contingencies. When the detail of security plans exceeds the available information, such plans become unconscionable maps.

Unconscionable Maps

The single paragraph long short story, "On Exactitude in Science" by Argentine author Jorge Borges describes an empire so advanced in cartography that its cartographer's guild "struck a Map of the Empire whose size was that of the Empire."[47] Future generations find they have little use for this excessive, "unconscionable map" and abandon the effort of their forefathers. All maps are abstractions. They are not the thing they represent, but are instead an explanation of it, an orientation or a statement of relationship to it. Unconscionable maps have forgotten they are not the territory and believe they represent all the territory. For security agencies, unconscionable maps take the form of the thousand page operational plan that remains unread by the first responder, or the unattainable presumption to a national, "near real-time situational awareness capability" for threats and hazards.[48] They are unreasonable or excessive not by being false, but by being incomplete and unaware of themselves.

Unconscionable maps have a tendency to pave over uncertainty—to render organizations insensitive to it by creating overly detailed scripts for uncertain futures. These are what Lee Clarke has called "fantasy documents," that is, documents that do not actually guide operations, but rather serve as reassurances that the organization has taken the problem seriously and stands ready to deliver.[49] Surveying planners deployed to Hurricane Sandy, FEMA found in 2013 that "64 percent either never used, nor had access to, regional hurricane plans."[50] This may simply be an area for improvement, as the FEMA after action report considered it. But it may cut both ways, indicating that there is an important and often overlooked distance between plans and operations, between organizational promise and organizational capability. If planners are failing to read plans, then perhaps plans are also failing to speak to planners. Schemes of prediction and preparation fall short of reality. Reflecting on the response to Hurricane Sandy, FEMA Administrator Fugate wrote, "We still plan for what we are capable of doing. We still train and exercise for what we can manage. We

must plan, train, and exercise even bigger to fracture the traditional mindset."[51]

Clarke emphasizes that planning, as a practice that makes a claim to expertise and knowledge about a given subject, is inherently political.[52] Organizations are often required to create plans for catastrophic contingencies, and Clarke stresses that such plans, as fantasy documents, are symbols of competence, claims that an organization has matters in hand. Such plans are not necessarily false, but not quite real either.

Organizations do not build their fantasy documents purely out of self-confidence. Such documents are often mandated by expectation. In 2013, Presidential Policy Directive 21 put forward a national goal of "near real-time situational awareness" of threats and hazards to critical infrastructure.[53] On its face, this is a remarkable pursuit. For companies that own infrastructure, such knowledge is often unattainable even at the facility level in many locations and industries. But in response to policies directing the pursuit of such absolute knowledge, homeland security organizations and agencies have cohered around methods for doing so--knowing it is not possible, they still pursue it. Claims to national "near real time" knowledge are, in this sense, unremarkable. They are supported by the large-scale organizational pursuit of those ends. And in one respect, this simply encourages the pursuit of excellence in risk management. Data collection and domain awareness do not necessarily suppose that all information can be known, but they have as their animating principle the idea that the more unlimited information collection capabilities and pursuits are, the better security will be. Unbounded risk, however, challenges this assumption with the grim idea that the information necessary to avert catastrophe will, by definition, only be revealed in catastrophe.

FEMA advises that emergency kits equip individuals and families for at least 72 hours.[54] There is little literature to suggest an origin for this three day minimum, less to bear out in practice its utility. There is no average disruption of 72 hours, no average catastrophic response or rescue time of 72 hours. It is, in short, largely arbitrary. It is a good idea, but no better than 100 or 200 hours of planned survival. It is a time frame invoked, rather than advised. The purpose of challenging this accepted number is not to discredit preparedness, but to highlight a tendency that security and planning practices have towards arbitrariness and presumptions of control. For this number surely communicates more than simply a lower bound of disaster. One will find the 72-hour number not just in guidance for individual readiness but also in guidance for incident responders. 72 hours is a benchmark for establishing incident command.[55] 72 hours is a time frame for initial planning assumptions, and the transition of operational control to field personnel.[56] What are we to make of catastrophe that extends beyond this mark? The symbolic nature of catastrophic plans is unavoidable—as we have seen, security agencies are given responsibility for impossible risks—but unconscionable maps present a secondary, self-imposed liability as organizations come to believe in their own fantasy documents.

Unconscionable maps are the unfortunate byproduct of the important work of applying risk calculation and carefulness to impossible security problems. Armed with such maps, however, agencies tasked with managing threats and catastrophes often claim to know and control more than is possible. This bias for imposed uniformity and presumed control is reflected not just in plans but also in operational doctrines.

Uniformity and Control

Unbounded risks have accelerated both precaution and the production of unconscionable security maps. At root, this is an effort to reduce uncertainty and thus increase control. It was this impulse that drove Guy Verhofstadft, the 47th Prime Minister of Belgium, to argue that, "borderless terrorism can only be tackled by borderless intelligence."[57] Global risks require global security governance. This springs from the sound observation that since risks will not conform to political or geographic boundaries, the means of managing risks must not do so either.[58] This impulse can take many forms—including more muscular, centralized national

security measures, or increasingly multilateral cooperation between nation state security services. In the U.S. the same impulses have led to the dominance of unilateral national preparedness doctrines.

First published in February of 2003, Homeland Security Presidential Directive 5 (HSPD-5) addressed the management of domestic incidents. Its purpose was succinct:

> [t]o enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.[59]

HSPD-5 directed the adoption of the National Incident Management System (NIMS) by all Federal agencies, and made NIMS a requirement for the receipt of Federal preparedness grants and contracts. By tying preparedness grant funding to the implementation of NIMS among grantees, FEMA commenced a disciplined shift toward "institutionalizing the use of [the Incident Command System (ICS)] across the entire response system," including non-federal responders.[60] Likewise, *The 9/11 Commission Report* recommended the adoption of ICS to "enhance command, control and communications capabilities."[61]

The stated purpose of NIMS is the provision of a "consistent nationwide template" for the management of all incidents—from house fires to catastrophic hurricanes and terrorist attacks.[62] The scope of the NIMS guidance is national in the classical sense; it is meant to apply equally to government and the private sector, to federal, tribal, state, municipal governments, and citizens. The central idea that underlies NIMS and ICS is to approach the uncertainty and complexity of incidents with regularity and order—to impose order upon chaos. Bearing the mark of the scientific management theories of Frederick Winslow Taylor and Henri Fayol, ICS was designed in the 1970s as a joint organizational model "built to accomplish the five basic functions of any successful organization: Command, Planning, Operations, Logistics, and Finance."[63] As an answer to unbounded risk, NIMS and ICS suppose that singularity, comprehensiveness, and the unification of all approaches under a common scheme are the answer to such risks. Standardization will permit seamless integration across disciplines and organizations. Uniformity will conquer chaos.

The scientific management approach of NIMS and ICS tends to resist rather than acknowledge the inherent complexity of incidents. The enduring complexity of catastrophe undermines the singular purpose of imposing order on chaos.[64] Such arrangements are designed for efficiency, not maneuverability. Like an assembly line, these systems do not respond well to change. However, after-action analysis following complex disasters is more likely to fault departments and agencies for insufficient organizational discipline than to suggest that NIMS is insufficiently adaptable.[65]

Considering "NIMS implementation behavior," Jessica Jensen observed that states and localities adopting NIMS as required for grant funding are modifying it heavily.[66] NIMS doctrine as written allows for a certain degree of local adaptation. The forms of adaptation taken at the implementation level nationwide are significant enough, however, that Jensen argues it may undermine the use of NIMS as the basis for national incident management. Perhaps more starkly than Jensen concludes, the extreme variability of approaches across jurisdictions undermines the usefulness of *any* national incident management model. National uniformity is an unconscionable map and perhaps fundamentally unachievable.

The intentionally inefficient system of federalism is the operating environment for domestic security. National security approaches like NIMS treat this network of governance as a liability. In the context of national preparedness, the efficiency of NIMS and ICS runs into a network of government intentionally designed to thwart the centralization of efficient power, and to recognize the disparities and rights of states.[67]

In a tactical sense, this creates enormous challenges around interoperability and coordination for crisis management. Central to the *9/11 Commission Report* recommendations was the call for interoperable communications and unified incident command structures.[68] Hesitance on the part of the federal government

influenced the Post-Katrina Emergency Management Reform act. More recently, after action reporting on the 2013 Navy Yard shooting in Washington, DC concluded that local and federal law enforcement failed to share key pieces of information such as the availability of live video within the building.[69] Such failures make uniformity appealing. They seem to support an argument for more standardization in operational capability, a more national approach to domestic crisis management, and perhaps even a single domestic preparedness agency. The tendency to impose such regularity, however, ignores the possibility that what is lacking is not a common system, but a common skill. While security agencies have labored unsuccessfully to impose unilateral doctrines and excessively detailed plans for contingencies, they have perhaps missed the starker lesson that in their current form security practices are not adaptable.

In his book *The Next Catastrophe*, Charles Perrow observes the tendency in modern systems—from infrastructure to bureaucratic management—towards centralization. Such centralization creates efficiencies, but also criticalities. Perrow highlights that the explosion of a single chlorine tanker outside of Los Angeles could poison 4 million people.[70] Likewise, the Metcalf substation attack of 2013 illustrated the high costs that can result from localized damage to high voltage transformers that "make up less than 3% of transformers in U.S. power substations," but "carry 60%-70% of the nation's electricity."[71] In the case of the Metcalf substation, a very inexpensive attack was able to create very expensive damage. A coordinated attack on multiple high voltage transformers might be much worse. Recognizing the liabilities of such centralization, Perrow emphasizes the need to deconcentrate, both in physical arrangements of systems and within organizations. Returning to the stark lesson of the Germanwings crash, centralizing the responsibility for 144 passengers with one pilot makes room for catastrophe. The fortress problem has relevant repercussions for physical security, infrastructure, and systems of management because it concentrates risk in the name of efficiency and control.

The prevailing narrative of threat and catastrophe response is not the disciplined deployment and coordination of known quantities, but rather the incorporation of uncommon partners to new circumstances. In this sense, a preparedness doctrine that embraced the network of federalism would recognize the inherent redundancy and resilience of a system that decentralizes strengths along with vulnerabilities. NIMS is ill-suited to this task. Rather than doubling down on scientific management, and engaging a unilateral doctrine of uniformity and control, homeland security requires an explicit doctrine of adaptability. High uncertainty risks may benefit from the strategic easing of fortifications.

The Unfortress

Some fortresses do not benefit from robustness alone. The next stage in the evolution of the American fortress requires a quantum shift from complication to complexity, and from robustness to adaptability.

For the Naskapi tribes in Canada, unpredictability was a matter of survival. The Naskapi followed the caribou, but the caribou were an adaptive adversary, responsive to the movements of hunters. The Naskapi turned to scapulimancy, a form of divination that relied on heating the shoulder blade of a caribou over a fire, and interpreting the cracks in its surface as auguries. Omar Khayam Moore contends that this magical practice effectively randomized Naskapi behavior, and served them as a tool for operating in conditions of uncertainty, outwitting their prey.[72] Regularity, control, and knowledge are not the best or only tools for navigating uncharted waters.

This may sound like so much barefoot philosophy, a pastoral fantasy, a pre-lapsarian vision of adaptable plans and nimble responders. But it is not intended to replace the current tangled approaches to complex problems with naïve simplicity. In his book *Learning from the Octopus*, Rafe Sagarin explores the ways that the DOD and DHS have created bureaucratic structures unable to respond rapidly to their threat environment. Part of his critique rests on comparing the predictive pursuits of security

organizations to the adaptability of evolutionary systems within nature. Evolution, says Sagarin, "proceeds by solving survival problems as they arise. Many systems in society, by contrast, are littered with meticulously planned designs—the Maginot Line comes to mind—that were entirely unable to solve emerging threats from the environment."[73] Organisms in nature survive without predictive knowledge because they have developed means of sensing and responding to changes in their environment. Many of the structures we put in place for the provision of security blunt our ability to respond to volatility in our environment. This is the danger of fortress thinking and focusing on solidity over adaptability, or prediction over agility. Unbounded risk makes such survival skills paramount. Assigned the unthinkable and the impossible, we are, in crucial and large-scale ways, responding with sclerotic, hardened tools designed for regularity. The measure of success for a security policy, capability, or approach should not be its solidity, but its mutability, not its robustness, but its agility. As crisis analyst Patrick Lagadec argues, "the problem is no longer about knowing the tools that help us to avoid surprises, but to train ourselves to be surprised."[74]

In the world of jazz performance "a fake-book is a bound collection of lead sheets…a musical score that shows only the melody of a work…"[75] Fake books provided the minimum necessary information about a song. Armed with fake books, jazz musicians could easily play the standards, and play them together. The ultimate form of the song and the solos would depend on the circumstance.[76] Fake books are form of melodic and harmonic crisis planning. Jazz performance relies on the interplay and communication between musicians as they improvise their way through a common theme. The results are unpredictable, and the essentials of the performance rely equally on the individual and technical proficiency of the musician, and his ability to keep time and communicate with the rest of the band. The written music for such unpredictable environments necessarily takes a form quite different from classical symphonic notation. Security agencies responding to complex risks may require fake book plans. Like the shoulder blades of the Naskapi, these plans are designed for change.

This is not to advocate for either divination or performance art in the sober business of security planning and operations. But the principles that inform such improvisational plans can be applied to planning for improbable catastrophes or dynamic environments. Threat and catastrophe have already begun to influence the way that FEMA plans for national contingencies. Facing unthinkable threats and hazards, FEMA has adopted a "Maximum of Maximums" approach to planning. Says FEMA Administrator Craig Fugate:

> [i]n emergency management we have only planned for what our capabilities can handle or only looked at what we can do to respond as government…But what we really need to be doing is planning for disasters that go beyond our capabilities. That's why we have to look beyond our government-centric approach and see what outside resources we can bring to the table.[77]

The maximum of maximums approach is effectively a "non-scenario." It is about coming to understand an organization at its limits, and learning to reach beyond them. It is not about the specific features of a given plausible future, or the actions an organization will take. Rather, like fake books, these plans are exercises in organizational self-knowledge, and preparation for the uncharted waters of catastrophe. Such plans are self-consciously incomplete and mutable by design. Caution and calculation are tempered with "a greater appreciation of limits and humility."[78] Plans may still need to be complicated, but that complication should not extend to excessively detailed scripts for imagined futures.

Plans are not the only complicated and robust fortresses that need to adapt. A provocative assertion went quietly unnoticed in 2014 outside of a narrow circle of risk management professionals. In its published white paper report entitled, "Quantifying U.S. Terrorism Risk" the firm Risk Management Solutions included the following assessment:

> [models of terrorism risk] tend to presume a lack of Western counter-terrorism capability to control terrorist action against the U.S. homeland. This presumption may be attributable to a dearth of public information about counter-terrorism activities. Counter-terrorism officials are duty-bound to "serve in silence." The whistle-blowing revelations of Edward Snowden have broken this code of silence, and by so doing have alerted the general public to the widespread and intensive surveillance undertaken to protect them from terrorist attack. Widespread public concern over this surveillance has provoked the NSA to publicly declare the importance of such surveillance in terrorist plot interdiction.[79]

For companies that build terrorism risk models, this is a sea change. The radical transparency of Edward Snowden's unlawful revelations allowed the insurance industry to better understand the mitigation in place against the terrorist risk. But the shift is even more provocative. According to Risk Management Solutions, terrorism risk can now be effectively modeled as a man-made catastrophe because "[c]arriers writing terrorism cover are insuring against the failure of a government's counter terrorism operations." In short, while the insurance industry is not ready to insure against terrorism without government financial backstops, they may be ready to insure against the government failing to be successful. In March of 2015, Pool Reinsurance Company Ltd.—the government backed insurance pool created by the British government in the wake of the Bishopsgate bombings in 1993—announced the purchase of terrorism reinsurance on the commercial market for the first time since its inception.[80] While the industry's ability to model terrorism losses has improved, its ability to predict terrorism has not. The insurance industry still views terrorism risks as a "constant, evolving and potentially expanding threat for the foreseeable future."[81] This is the adaptation of a modern fortress.

Conclusion

Joint intelligence products developed through the Office of the Director of National Intelligence often remind the reader that many suspicious activities are constitutionally protected behaviors. Another way of expressing this reality is that democratic society is not designed to be unreasonably safe.

John Witherspoon, long time president of what would become Princeton University, signer of the Declaration of Independence, and teacher to many of the American founding fathers, considered theoretically what it meant for a nation to provide "reasonable security."[82] Witherspoon recognized that absolute security might be totalitarian and was impossible anyway. It is a considerable irony that 18th century governmental theory should display such cold realism, while current national preparedness doctrine reflects a utopian confidence:

> [a] secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.[83]

It may be semantic scolding to observe that a nation in possession of the capabilities to prevent all threats and hazards need not worry about responding to them. But it may also indicate that security agencies have lost the ability to understand themselves in terms of the provision of reasonable security. Security agencies may be in pursuit of unreasonable security, implicitly promising more than they can provide.

Faced with expanding uncertainty, security agencies have sought expanded predictability. Faced with complexity, they have sought regularity. Wrestling with disparate arrangements across jurisdictions and sectors, security efforts have sought to build national uniformity. However, uncertainty endures, complexity seems inevitable, and American government was designed specifically to resist the centralization of efficient power, uniform national systems of crisis management, or the centralized command of resources during disasters. It is the inherent nature of unbounded risks to defy efforts at uniformity and control. In one sense, this is simply to recognize

that the margin of what remains unknown is of particular import to homeland security agencies and efforts. The unlikely rail accident, the unthinkable airline crash, and the worst case earthquake or pandemic are specifically the province of agencies and organizations responsible for national preparedness. The poet Walt Whitman "dream'd in a dream" of "a city invincible to the attacks of the whole of the rest of the earth."[84] Perfect security remains as Whitman saw it, a dream.

However, the national capabilities and approaches currently in use are not optimized for the management of outliers or for living with unbounded risks. Designed around assumptions of threat, vulnerability, and consequence, the architecture of homeland security decision-making is less attuned to situations where this information is unavailable. In this environment it is difficult to know how much safer security efforts make America.

Centralization and efficiency have a curious revenge effect—they also create vulnerabilities. Understanding that the tragedy of Germanwings 9525 was made possible by robust and complicated fortification means recognizing that the centralization, even of strengths, makes room for unbounded risk. Distributing both vulnerabilities and strengths means embracing the network of federalism. Abandoning the pursuit of NIMS, or the command and control doctrines of ICS is an unlikely proposition, and yet the dynamic nature of modern risk may require it. Inheriting unbounded risk may mean turning away from the manufactured insecurities that accompany unconscionable maps, and toward a better means of living with and adapting to danger.

A grand design for homeland security will not produce grand security. Homeland security agencies require fewer scripted plans and more improvisation, more diversity, less uniformity, less training with partners and more learning to work with strangers. These things will make us safer, but they will not make us safe.

About the Author

Jack Anderson *is a senior analyst at the Department of Homeland Security's National Protection and Programs Directorate. He has a background in insurance investigation, catastrophe and crisis response, post-disaster forensics, risk management, infrastructure security, and doctrine development. He holds an M.A In Security Studies from the Naval Postgraduate School (2015) and a B.A in English from Grove City College (2004). He is the book reviews editor for hs-community.org and his writing has appeared in the Wall Street Journal and other publications. He may be reached at jacob.anderson@hq.dhs.gov*

Disclaimer

The views expressed here are solely the author's and do not reflect the views of the Department of Homeland Security or the National Protection and Programs Directorate.

Notes

1. Eugène-Emmanuel Viollet-le-Duc, *Dictionnaire raisonné de l'architecture française du XI au XVI siècle* [dictionary of French architecture from the 11th–16th century] (Paris, FR: A. Morel, 1869), 296.

2. Bureau d'Enquêtes et d'Analyses pour la Sécurité de l'Aviation Civile (BEA), *Rapport préliminaire Accident survenu le 24 mars 2015 à Prads-Haute-Bléone (04) à l'Airbus A320-211 immatriculé D-AIPX exploité par Germanwings* [Preliminary Report on the Germanwings Flight 9525 Crash] (Paris, FR: BEA, May, 2015), 11. The French government provided an English translation of the preliminary report as a courtesy, however the original French language version cited contains the official report language.

3. Even industry standards in the U.S, which require two people in the cockpit at all times, do not contemplate the possibility of two aggressors in the cockpit. The cockpit door locking system and entry keypad on the Airbus a320 (involved in the Germanwings 9525 crash) is designed to allow flight crew outside the cockpit to enter if the door is locked, unless the flight crew in the cockpit prevents them. U.S. regulation and industry rules require two crewmembers in the cockpit at all times, but at the time, European regulations did not. See Flight crewmembers at controls, 14 C.F.R §121.543 (2013); Jon Ostrower, "United Shifts Two-Crew Cockpit Policy on Certain Boeing Jets," *Wall Street Journal* (March 27, 2015), sec. Business.

4. EASA Safety Information Bulletin SIB No.: 2015-04 Issued: 27 March 2015. Transport Canada, along with New Zealand Civil Aviation Authority and Australian airlines followed suit in 2015.

5. Ulrich Beck, "Living in the World Risk Society," *Economy and Society* 35, no. 3 (August 1, 2006): 329–45.

6. Eugène-Emmanuel Viollet-le-Duc, *Annals of a Fortress*, translated by Benjamin Bucknall, (Boston, MA: J. R. Osgood and Company, 1876).

7. Ibid., 359.

8. Kenneth C. Fletcher, "Aviation Security: A Case For Risk-Based Passenger Screening," (master's thesis, Naval Postgraduate School, 2011).

9. Ashley Halsey III, "TSA Tightens Security amid Discovery of Airport Gun Smugglers," *Washington Post*, July 14th, 2015. Accessed August 4, 2015.

10. Department of Homeland Security, Office of Inspector General, *TSA Can Improve Aviation Worker Vetting* (Redacted), OIG-15-98 (Washington, DC: June 4, 2015).

11. Henry Samuel, "France to Authorise 'Military Intervention against ISIL' on Home Soil," November 4, 2015, sec. World, http://www.telegraph.co.uk/news/worldnews/europe/france/11976042/France-to-authorise-military-intervention-against-Isil-on-home-soil.html.

12. Jack Davis, "Strategic Warning: If Surprise is Inevitable, What Role for Analysis?" The Sherman Kent Center for Intelligence Analysis, Occasional Papers: Volume 2, Number 1 (Washington, DC: January 2003).

13. Zhuangzi, *The Complete Works of Zhuangzi*, translated by Burton Watson, Translations from the Asian Classics (New York, NY: Columbia University Press, 2013), 281.

14. Ulrich Beck, "Living in the World Risk Society," *Economy and Society* 35, no. 3 (August 1, 2006): 329–45.

15. Todd Mass, Siobahn O'Neil, and John Rollins, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress* (CRS Report No. RL33858) (Washington, DC: Congressional Research Service, 2007), Summary, http://www.fas.org/sgp/crs/homesec/RL33858.pdf.

16. Department of Homeland Security, *U.S. Department of Homeland Security Agency Financial Report Fiscal Year 2014* (Washington, DC: DHS, February 2015).

17. Douglas Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It* (New York, NY: John Wiley and Sons, 2009), 8; Lee Clarke, *Mission Improbable: Using Fantasy Documents to Tame Disaster* (Chicago, IL: University of Chicago Press, 1999), 11.

18. Ian Hacking, *The Taming of Chance, Ideas in Context* (New York, NY: Cambridge University Press, 1990), vii.

19. Greg Miller and Adam Goldman, "Terrorist Plot Exposes Blind Spot for U.S. Authorities," *The Washington Post*, December 4, 2015, https://www.washingtonpost.com/world/national-security/terrorist-plot-exposes-blind-spot-for-us-authorities/2015/12/04/6e473e0e-9aa4-11e5-8917-653b65c809eb_story.html?hpid=hp_hp-top-table-main_isis713pm%3Ahomepage%2Fstory.

20. Peter Baker and Eric Schmitt, "California Attack Has U.S. Rethinking Strategy on Homegrown Terror," *The New York Times*, December 5, 2015, http://www.nytimes.com/2015/12/06/us/politics/california-attack-has-us-rethinking-strategy-on-homegrown-terror.html.

21. Adrian Kent, "A Critical Look at Risk Assessments for Global Catastrophes," *Risk Analysis* 24, no. 1 (2004): 157–68.

22. Department of Homeland Security, Office of the Inspector General, *FEMA and the State of Louisiana Need to Accelerate the Funding of $812 Million in Hazard Mitigation Grant Program Funds and Develop a Plan to Close Approved Projects* (Washington, DC: DHS, September, 2014).

23. Lee Clarke, *Worst Cases: Terror and Catastrophe in the Popular Imagination* (Chicago, IL: University of Chicago Press, 2006), 44.

24. "Lufthansa, Air France Avoid Flying over Sinai after Crash," Reuters, October 31, 2015, http://www.reuters.com/article/us-egypt-crash-airlines-idUSKCN0SP0W220151031.

25. Cass Sunstein, *Laws of Fear: Beyond the Precautionary Principle, John Robert Seeley Lectures* (New York, NY: Cambridge University Press, 2005), 224.

26. Cass Sunstein, "The Paralyzing Principle," *Regulation* 25, no. 4 (Winter 2002/2003 2002): 32.

27. Nassim Nicholas Taleb, et al., "The Precautionary Principle (with Application to the Genetic Modification of Organisms)," *Extreme Risk Initiative* (New York, NY: NYU School of Engineering Working Paper Series, September, 2014).

28. Cass Sunstein, "The Paralyzing Principle."

29. Claudia Aradau and Rens Van Munster, "Governing Terrorism through Risk: Taking Precautions, (un)Knowing the Future," *European Journal of International Relations* 13, no. 1 (2007): 89–115.

30. Charlie Savage, "Surveillance Court Rules That N.S.A. Can Resume Bulk Data Collection," *The New York Times*, June 30, 2015. http://www.nytimes.com/2015/07/01/us/politics/fisa-surveillance-court-rules-nsa-can-resume-bulk-data-collection.html.

31. Paul Ryan, "Paul Ryan: On Refugees, Balance, Safety, Compassion - CNN.com," *CNN*, accessed December 4, 2015, http://www.cnn.com/2015/11/23/opinions/ryan-syrian-refugees/index.html.

32. Ibid.

33. Department of Homeland Security, *DHS Budget-In-Brief Fiscal Year 2016* (DHS, Washington, DC: 2015), 2.

34. "TSA Detected Record Number of Firearms at Checkpoints in 2015," *Transportation Security Administration*, January 21, 2016, https://www.tsa.gov/news/releases/2016/01/21/tsa-detected-record-number-firearms-checkpoints-2015.

35. John Mueller, and Mark Stewart. "Hardly Existential," *Foreign Affairs* (April 2, 2010).

36. Howard Kunreuther, and Erwann Michel-Kerjan, *TRIA after 2014: Examining Risk Sharing under Current and Alternative Designs* (Philadelphia, PA: Wharton, University of Pennsylvania, 2014); Milken Institute, *The Impact of September 11 on U.S. Metropolitan Economies* (Jan. 2002).

37. "Testimony on TSA Efforts to Address OIG Findings," *Transportation Security Administration*, September 29, 2015, https://www.tsa.gov/news/testimony/2015/09/29/testimony-tsa-efforts-address-oig-findings.

38. Sunstein, *Laws of Fear: Beyond the Precautionary Principle,* 24.

39. "The Japanese Mayor Who Was Laughed at for Building a Huge Sea Wall - until His Village Was Left Almost Untouched by Tsunami," Mail Online, May 14, 2011, http://www.dailymail.co.uk/news/article-1386978/The-Japanese-mayor-laughed-building-huge-sea-wall--village-left-untouched-tsunami.html .

40. John Rawls, *A Theory of Justice* (Boston: Harvard University Press, 2009), 133.

41. Sunstein, *Laws of Fear: Beyond the Precautionary Principle*, 224.

42. National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York, NY: W.W. Norton & Company, 2004), 344.

43. Michael Barkun, "Defending Against the Apocalypse: The Limits of Homeland Security," *Policy Options* (September 2002).

44. Lloyd's and the University of Cambridge Centre for Risk Studies, *Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid, Emerging Risk Report 2015, innovation series* (London, UK: 2015).

45. Homeland Security Council, *National Planning Scenarios: Executive Summaries Created for Use in National, Federal, State, and Local Homeland Security Preparedness Activities* (Washington, DC: Homeland Security Council, April, 2005).

46. H.R.3410-Critical Infrastructure Protection Act, 113th Congress (2013-2014). Apparently unbeknownst to the authors of H.R 3410, the national planning scenarios were rescinded in 2011 with the institution of Presidential Policy Directive 8 (PPD-8), which replaced HSPD-8. This detail would make H.R 3410 either very easy, or very difficult to implement if it were to pass the Senate.

47. Jorge Louis Borges, *Jorge Luis Borges, Collected Fictions,* translated by H. Hurley (New York, NY: Penguin Books, 1998), 235.

48. White House, *Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience* (Washington, DC: White House, February 12, 2013).

49. Clarke, *Mission Improbable*, 73.

50. FEMA, *Hurricane Sandy FEMA After Action Report* (Washington DC: July 1, 2013), 15.

51. Ibid., i.

52. Ibid., 13.

53. White House, Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience (Washington, DC: White House, February 12, 2013).

54. Federal Emergency Management Agency, "Build a Kit." Last Accessed August 1, 2015. http://www.ready.gov/build-a-kit.

55. FEMA, *Hurricane Sandy FEMA After Action Report* (Washington DC: July 1, 2013), 14.

56. Ibid.

57. Guy Verhofstadt, "Borderless Terrorism Can Only Be Tackled by Borderless Intelligence," *The Guardian*, November 16, 2015, http://www.theguardian.com/commentisfree/2015/nov/16/terrorism-intelligence-paris-europe-security-services.

58. Ulrich Beck, "The Terrorist Threat World Risk Society Revisited," *Theory, Culture & Society* 19, no. 4 (August 1, 2002): 39–55.

59. White House, *Homeland Security Presidential Directive 5: Management of Domestic Incidents* (Washington, DC: February 28, 2003).

60. "New Position Paper on National Incident Management System (NIMS) Incident Command System (ICS) - Homeland Security Digital Library Blog." Accessed April 16, 2015.

61. National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York, NY: W.W. Norton & Company, 2004), 397.

62. Federal Emergency Management Agency, *National Incident Management System* (Washington, DC: FEMA, December 2008), i.

63. Frederick Winslow Taylor, *The Principles of Scientific Management* (New York, NY: Harper, 1913), 10; Henri Fayol, *General and Industrial Management* (London, UK: Pitman, 1949); Kimberly S Stambler and Joseph A Barbera, "Engineering the Incident Command and Multiagency Coordination Systems," *Journal of Homeland Security and Emergency Management* 8, no. 1. (January 23, 2011).

64. Dick A. Buck, Joseph E. Trainor, and Benigno E. Aguirre, "A Critical Evaluation of the Incident Command System and NIMS," *Journal of Homeland Security and Emergency Management* 3, no. 3 (2006).

65. FEMA, *Hurricane Sandy FEMA After Action Report* (Washington, DC: July 1, 2013), 12.

66. Jessica Jensen, "The Current NIMS Implementation Behavior of United States Counties," *Journal of Homeland Security and Emergency Management* 8, no. 1. (January 2, 2011).

67. Alexander Hamilton, James Madison, and John Jay, *The Federalist Papers* (Mineola, NY: Dover Publications, 2014), 186.

68. National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, 397.

69. Metropolitan Police Department of Washington DC, *After Action Report Washington Navy Yard September 16, 2013 Internal Review Of The Metropolitan Police Department* (Washington, DC: July 2014), 53.

70. Charles Perrow, *The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters* (Princeton, NJ: Princeton University Press, 2011), 188.

71. Paul W. Parfomak, *Physical Security of the U.S. Power Grid: High-voltage Transformer Substations* (Congressional Research Service, Washington DC: June 17, 2014), 1.

72. Omar Khayyam Moore, "Divination-A New Perspective," *American Anthropologist*, New Series, 59, no. 1 (February 1, 1957): 69–74.

73. Rafe Sagarin, *Learning From the Octopus: How Secrets from Nature Can Help Us Fight Terrorist Attacks, Natural Disasters, and Disease* (New York: Basic Books, 2012), xxiii.

74. Patrick Lagadec, "Risks and Crises in Terra Incognita", *ParisTech Review*, October 11, 2010, http://www.paristechreview.com/2010/10/11/risks-crises-terra-incognita/.

75. Rebecca Koblick, "Jazz Fake-books as a Resource in the General Library," *Collection Building* 32, no. 4 (2013): 139-144.

76. Fake books were also subversive documents. The best of them were illegally produced in violation of copyright, providing basic information about a wide range of musical numbers.

77. FEMA News Desk, "Release 101020: FEMA Administrator Craig Fugate Urges State Emergency Managers To Prepare For The Worst And Consider The Entire Community While Planning For Disaster, No.: HQ-10-203" (Washington, DC: October 20, 2010).

78. Clarke, *Worst Cases*, 183.

79. Risk Management Solutions, *Quantifying U.S. Terrorism Risk, White Paper* (Newark, CA: RMS, 2014), 8.

80. "Pool Re Purchases £1.8 Billion in Reinsurance," PoolRe, Accessed March 9, 2015, https://www.poolre.co.uk/pool-re-purchases-1-8-billion-in-reinsurance/.

81. Robert P. Hartwig and Claire Wilkinson, *Terrorism Risk: A Constant Threat, Impacts for Property and Casualty Insurers,* Paper (New York, NY: Insurance Information Institute, March 2014), 5.

82. John Witherspoon, *The Works of John Witherspoon, D.D* (Edinbourgh, SCT: Ogle and Aikman, J. Pillans, J. Ritchie, J. Turnbull, 1805), 111.

83. Department of Homeland Security, *National Preparedness Goal, First Edition* (Washington, DC: DHS, September, 2011), 1.

84. Walt Whitman, *Leaves of Grass Including a Facsimile Autobiography, Variorum Readings of the Poems and a Department of Gathered Leaves*, Edited by David McKay (Philadelphia, US: David McKay, 1891-1892), 109.