

## **On Vital Systems Security**

Stephen J. Collier and Andrew Lakoff

Presentation at the University of Helsinki Collegium

June 2008

### ***Draft – Not for Citation***

In the past few years we have been engaged in a project on the rationalities, techniques and objects of contemporary security expertise. Our work has been part of a collaborative project, which combined individual research with collective reflection on concepts and problems.

We started from an interest in new organizations and strategic concepts related to security in the United States, such as critical infrastructure protection, the Department of Homeland Security, preparedness, and biosecurity. These organizations and initiatives have featured centrally in discussions of national security. But they do not deal with threats from conventional foreign enemies. Rather, they are concerned with uncertain future events such as pandemic disease, terrorist attacks, or natural disasters. They do not aim to deter or prevent these events but rather to mitigate their impact by organizing preparedness for response and recovery and by reducing the vulnerability of critical systems potentially affected by these threats – health systems, transport and energy infrastructures, economic mechanisms. Some of the questions we have tried to address in this project are: How can we think about the significance and novelty of these forms? How do they relate to prior approaches to national security? Or to social welfare and economic management – the domains in which concern for these “critical infrastructures” of domestic life usually fall?

Our approach to investigating these questions has drawn on Michel Foucault’s genealogical work on different ways of “problematizing” security, that is, different ways

of understanding and managing threats to collective life. In *Security, Territory, Population*, Foucault described the rise of a new form of security focused on the well-being of populations that was distinct from the existing form of sovereign state security. Sovereign state security, which dates to the rise of the modern territorial state, is concerned with state integrity in the face of foreign and domestic threats. Its principle apparatuses of warfare and diplomacy are oriented to maintaining sovereign power, whether that is understood to inhere in a monarch or in a group of legal subjects. By contrast, what Foucault called the “security of populations,” which took shape in the mid-18<sup>th</sup> to early 19<sup>th</sup> century, deals not with external enemies, but with the regularly occurring “pathologies” of collective life: disease, poverty, and crime, for example. Foucault argued that population security was based on what he called an “entirely new economy of power,” one that operated not on legal subjects but on living beings. This form of security gave rise to a series of new governmental apparatuses – public health, social welfare, and economic regulation – through which life and population were taken up as political problems, and objects of collective security. This process was central to what Foucault called “the birth biopolitics.”

We initially sought to understand new security initiatives in terms of these two existing technologies of power. However, for reasons that we will describe in this talk, we gradually came to think that they were better understood in relation to a novel form of security – what we call “vital systems security.” Vital systems security is a way of “problematizing” threats to security that can be contrasted to the forms of sovereign state security and population security. Vital systems security takes up events that are uncertain and unpreventable but potentially catastrophic. Its object of protection is the complex of

critical systems or networks on which modern economies and polities depend. The normative rationality of vital systems security is oriented to the resilience of these systems, and preparedness for response to events that might disrupt them. Finally, vital systems security deals with the population insofar as it is dependent on these vulnerable, vital systems. Vital systems security is in this sense to “reflexive modernization” in Beck’s sense – the idea that the very success of industrial and social modernity in managing risks has in fact generated new risks.

	<b>Sovereign State Security</b>	<b>Population Security</b>	<b>Vital Systems Security</b>
<b>Object of Protection</b>	Territorial sovereignty	The population	Vital system, critical infrastructure
<b>Way of constituting “event” or threat</b>	Enemy attack, based on strategy and capabilities	Regularly occurring pathologies of the social field	Unpredictable, undeterrable, potentially catastrophic
<b>Normativity</b>	Prevention, deterrence through military superiority	Health, welfare	Resilience, preparedness for response
<b>Relation to population</b>	Population as collection of legal subjects	Population as domain of regularly occurring processes	Population as dependent on vulnerable PS systems

In this talk we will outline some elements of the genealogy of vital systems security to show how this distinctive style of reasoning about security problems has been linked to increasingly potent techniques and robust organizations. First, we outline a schematic story of the mid-to-late-20<sup>th</sup> century development of vital systems security – focusing on some fairly obscure episodes and sites: the development of strategic bombing in the U.S. Air Corps Tactical School between the World Wars; the rise of post-World War II civil defense; and the invention of new approaches to managing systems

vulnerability in the Office of Emergency Preparedness in the 1960s and early 1970s. We will also try to offer some indication, in the second part of the presentation, of how the techniques and styles of reasoning developed in these sites have been redeployed outside of superpower confrontation: from terrorism to energy crises, from natural disasters to pandemic disease.

A qualification should be made at the outset. Following Foucault’s admonition in *Security, Territory, Population*, we do not mean to suggest that there has been an epochal shift from population security or sovereign state security to vital systems security – or that VSS is the dominant paradigm of security today. Rather, our point is that techniques oriented to securing vital systems have become increasingly significant as possible responses to security problems – often in combination, or in tension, with other forms of security.

### **Vital Systems as a Military Problem**

The genealogy of vital systems security can be traced back along various lines. For example, as Timothy Mitchell has shown, the *object* of vital systems security was identified by early 20<sup>th</sup> century industrialists facing strikes that could disrupt key nodes in chains of industrial production. In response, we see an early effort to think about the economy not in terms of productivity and wealth but as a collection of vulnerable, vital systems. Alternately, the distinctive way of treating *events* in vital systems security – as uncertain future catastrophes not “knowable” through analysis of past events – is found beginning in the 1930s when insurance experts took initial steps in establishing an actuarial framework for assessing earthquake risk.

But the most important area for the initial development of the concepts and techniques of vital systems security was military conflict and military preparedness, the classic domains of sovereign state security. In particular, this development was linked to a specific moment in the history of warfare, when the paradigm of sovereign state security was undergoing a significant transformation related to the rise of total war. Total war, of course, involves the systematic incorporation of the national economy and population into the war effort – in other words, it was one intersection between population security and sovereign state security. But it was simultaneously a context in which national economies began to be rethought as collections of vital systems.

In the 19<sup>th</sup> century, total war was associated with the advent of national armies and mass conscription. But by the beginning of the 20<sup>th</sup> century, it referred to a form of warfare that enlisted the full resources of a country – including its productive apparatus – into military effort. This new form of *industrialized* total war consolidated during World War I, when all the major combatants introduced new forms of economic planning and coordination – particularly of energy, critical materials, and manufacturing – to contribute to the war effort. This development opened a significant new horizon of strategic thinking for military planners. If national populations and domestic economies were key instruments of warfare, then they could also be conceived as strategic targets. In the waning months of World War I, and then with increased intensity during the interwar period, this new understanding of the domestic economy and polity – as a key instrument of war and thus as target of attack – was developed in the theory of strategic bombing.

After World War I, there were two distinct schools of strategic bombing. One focused on “terror” bombing that targeted civilians in order to break their will to

contribute to the war effort. The other, which explicitly rejected terror bombing, introduced a different rationale for air war: not to attack enemy forces or civilian populations, but to attack the industrial systems, and the transport and energy infrastructures, upon which an enemy's war effort depended. Theorists of this second approach developed a new understanding of the national economy – as an interlinked network of critical systems that might be disrupted through air attack. One important locus for developing this new understanding was the U.S. Air Corps Tactical School, the most important institution in the development of strategic bombing in the United States.



*Air Corps Tactical School, Map Problem Room*

Theorists at ACTS began to think of enemies not in terms of their military forces and capabilities but in terms of the productive capacities and infrastructural networks that were necessary for the enemy to engage in full-scale war. They focused in particular on

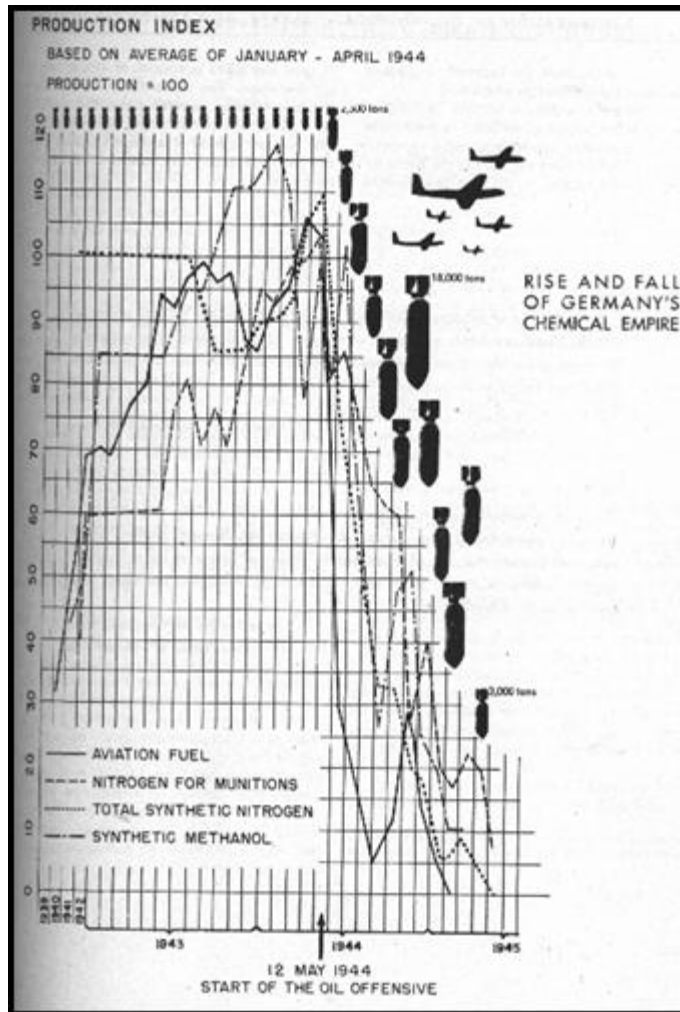
“choke points” or “vital nodes” – key factories, transport arteries, and energy systems – that, if destroyed, could disrupt important parts of an enemy’s industrial system. In doing so, they outlined a new way to “know” national economic systems: not in terms of productivity and welfare – the concerns of population security – but in terms of their *vulnerability* to attack and disruption. It is worth noting here that the qualifier “vital” was widely used in military discussions to designate targets or objectives that were critical to strategic goals. With strategic bombing, “vital” came to bear an additional meaning, referring to the systems upon which society and economy depend.

The emphasis on targeting ‘vital nodes’ was important in formulating U.S. air strategy during World War II, although there is dispute about its effectiveness. Moreover it should be distinguished from the more well-known U.S. air war strategy of carpet bombing. Here, however, our concern is just to illustrate the style of reasoning found in an approach to strategic bombing oriented to disrupting an economy’s vital systems. In some cases, it was used to aim at targets that were vital to a specific theater of battle. For example, before and during D-Day the Allied forces carried out a Transportation Plan that targeted specific sites such as the Juvisy Train Yards, pictured here before and after aerial bombing. The vulnerable, vital system, in this case, was a local node in a transportation network used for moving materiel and troops to an active front. In other cases, vulnerability was conceived in terms of entire economic sectors, for example in the Allied campaign to destroy the German chemical industry.



*Juvisy Train Yards, before and after aerial bombing*

This chart from the United States Strategic Bombing Survey, which reviewed the effects of strategic bombing after the war, shows the relationship between output of key chemical products and total tonnage of allied bombing in the “oil offensive” campaign. By destroying key factories or sources of inputs, a broad part of a war economy could be disabled. What is of interest here is that an entire sector of the German economy – articulated by a collection of enterprises and transportation systems – could be constituted as an object of knowledge and as a vital target. In strategic bombing, thus, we see a new understanding of the national economy – as a collection of vital systems that are vulnerable to disruption.

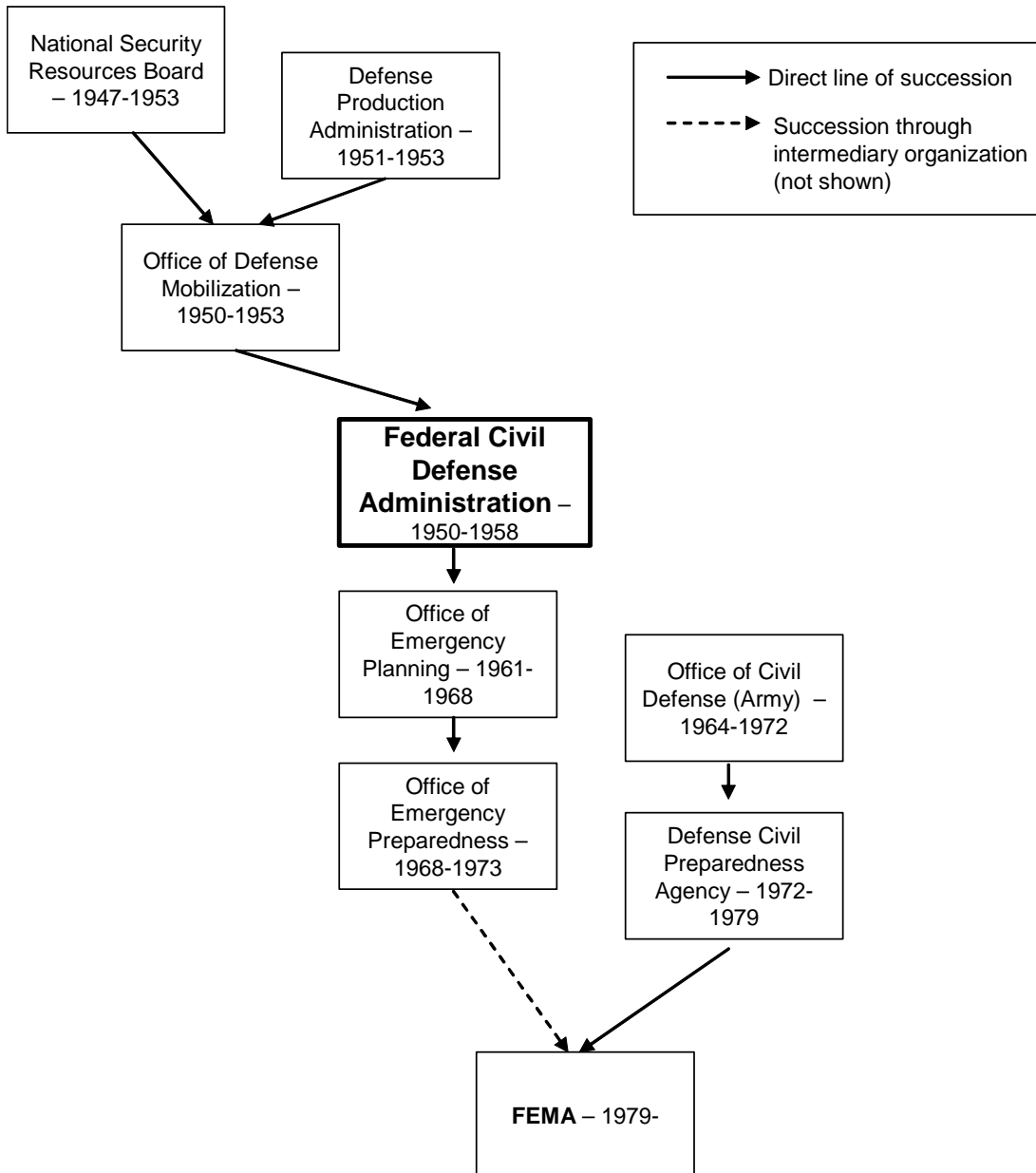


*“Rise and Fall of Germany’s Chemical Industry”  
United States Strategic Bombing Survey*

### **The Vulnerable Homeland**

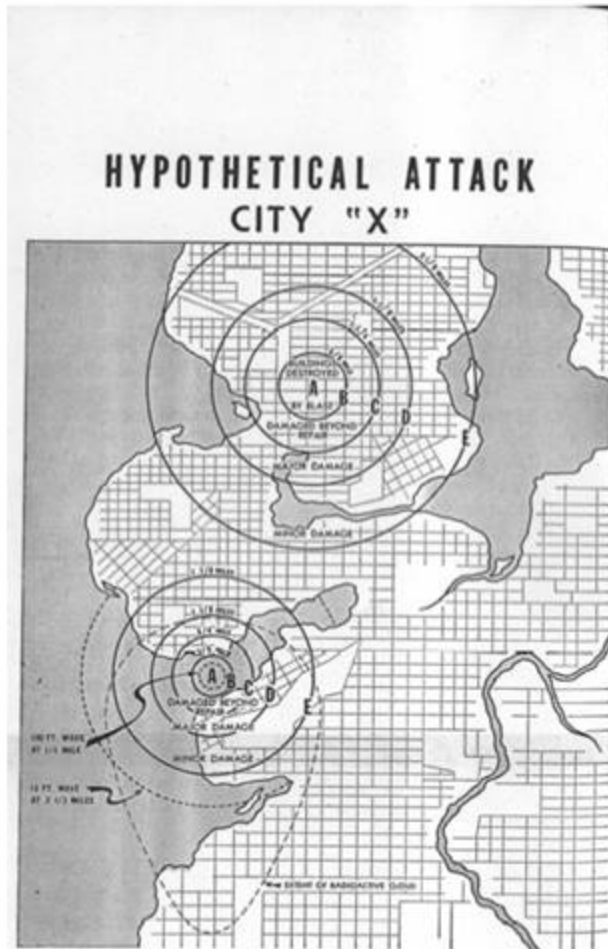
Let us turn now to a second point of inflection in the genealogy of vital systems security, through which this approach to thinking about the enemy was transposed onto the U.S. as itself a target of strategic bombing. This shift took place after World War II, with the rise of the Cold War and the nuclear era. Two domains of security planning and organization were particularly important in this development. The first, civil defense, was concerned primarily with the protection of civilian populations. The second, defense mobilization, was concerned with assuring that the U.S. economy could sustain the level

of industrial production required for the conduct of war, even, potentially, after a nuclear attack. If strategic bombing theorists asked how national economies could be conceived as a target, then civil defense and defense mobilization planners asked how it could be conceived as an object of protection.



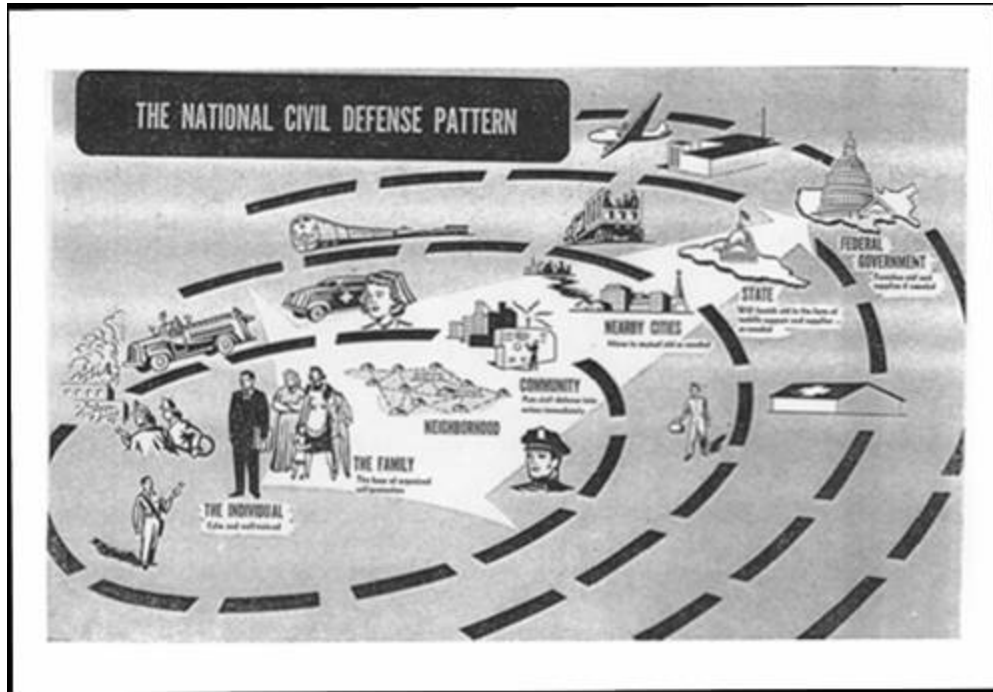
*Organizations Involved in U.S. Emergency Response and Defense Mobilization*

Let us turn first to civil defense planning, which, beginning in 1949, was conducted by the U.S. Federal Civil Defense Agency. In civil defense a number of important techniques and organizational forms were developed that were crucial in the evolution of vital systems security. For example, civil defense planners developed techniques of “catastrophe modeling” to understand the effects of nuclear detonations in cities. They began with spatial models of nuclear detonations, which indicated the dispersion of “blast effects,” firestorms, and radiation over a certain geographical locale. On the same map planners placed structures and other features such as roadways or communication systems that would be affected by the event. By combining these two elements – initially through very rudimentary methods employing transparent overlays – civil defense planners could produce a “vulnerability map.” Through such maps apparatuses of population security were problematized in a new way. Water systems, transportation networks, social services and emergency response organizations – all initially created to promote health and welfare, and to deal with regularly occurring social pathologies of disease, crime, and poverty – were understood in terms of their vulnerability to attack, and in terms of their role in post-attack response. Here, again, we have a fundamentally new kind of knowledge about collective life: not a statistical analysis of actual prior events but enacted knowledge about potential future events. Such techniques of enactment have played a central role in the subsequent development of vital systems security, from imaginative scenarios to highly formal catastrophe models.



In civil defense, the most important function of vulnerability maps was to plan for emergency response. Civil defense officials recognized that various organizations not normally involved in managing large emergencies – such as public health services, police, and social service departments – would be crucial to post-attack response. They also realized that these local organizations would not be able to cope with an emergency on their own, and would require assistance both from other localities and from state and regional governments. In the U.S., civil defense authorities defined a distinctive organizational form for response planning that adapted the structures of U.S. federalism to new challenges presented by the prospect of nuclear war. Assuming that the capacities of local governments would be overwhelmed in the event of a nuclear attack, they

organized patterns of emergency coordination between cities, states, and the federal government. They also applied a series of military preparedness techniques – such as exercises and contingency planning – to domestic emergency response. Thus, we see in civil defense another key element found in subsequent articulations of vital systems security: an apparatus of domestic “distributed” preparedness.



### **System Vulnerability**

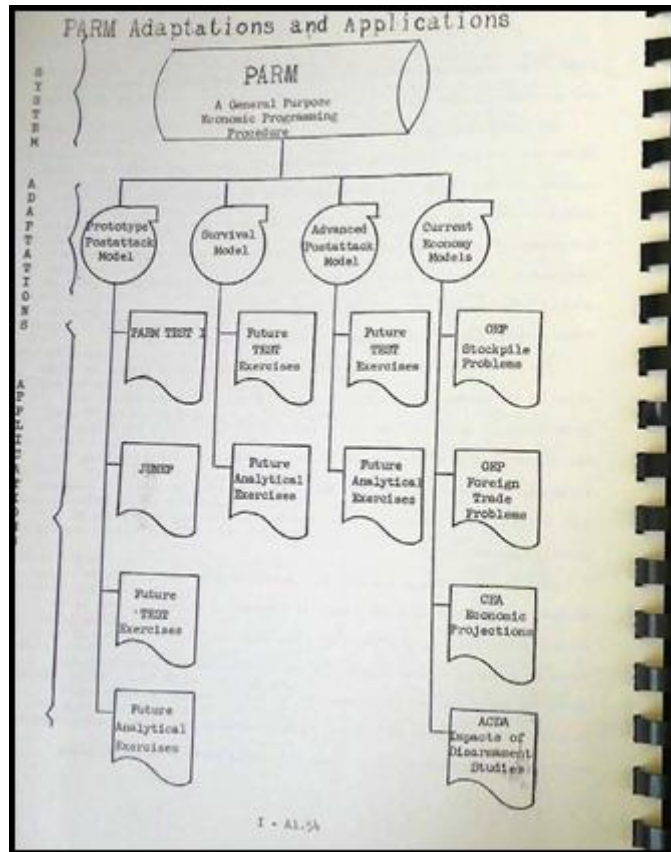
In Cold War civil defense planning, vulnerability mapping and emergency response were geared to the relatively local effects of a specific catastrophic event – the detonation of a discreet bomb in a U.S. city. Techniques for modeling such “local” detonations became more sophisticated through the 1950s, particularly as defense planning agencies employed computer models that could take into account patterns of weather and population movement that would affect both the immediate impact of a nuclear detonation and preparedness requirements

During the 1960s, however, we observe a significant shift in US civil defense and mobilization planning. Civil defense strategists and technicians turned their attention from modeling single nuclear explosions in a given city to modeling complex attack scenarios – potentially involving many detonations – in order to understand their impact on the vital systems of the U.S. as a whole.

An important site for these developments was the Office of Emergency Planning, a federal agency founded in 1962. OEP was one successor organization to the U.S. Civil Defense Administration, and it inherited civil defense concerns with modeling catastrophes and with developing techniques for response preparedness. But OEP's mission extended beyond civil defense. The executive order establishing the office identified civil defense – focused on reducing civilian mortality – as only one function of domestic emergency preparedness. Another set of problems taken up by OEP were related to “defense production.” Defense production was concerned with a central problem of total war: that the U.S. maintain the capacity to produce the strategic inputs required for an industrial war economy. But after World War II, with the rise of the air-nuclear age, the officials and technicians in organizations like OEP became preoccupied with the vulnerabilities of these systems. The question, then, was not just whether the U.S. had the productive capacity required to conduct war, but whether, as a 1962 OEP report noted, the U.S. could "achieve a mobilization base for whatever contingencies are determined to obtain." In this light, OEP took up the problem of knowing the economy in a new way – as a complex of vital systems.

The task of modeling the effects of nuclear war on the broader system of industrial production in the United States was taken up by the National Resource

Evaluation Center, a division of OEP that focused on the mathematical analysis of resource availability using new computing capabilities. NREC was founded in 1957, and in the early 1960s was working on so-called “survival models” that simulated the condition of the U.S. economy after a nuclear attack. These survival models were a kind of vulnerability mapping. But rather than focusing on a single detonation in a specific city – as in civil defense planning – they simulated attack patterns over the entire U.S. economy, examining specific sectors both individually and in their complex interdependence. Here, to offer just a glimpse of how these models were assembled, is a diagram of the PARM model. PARM was a major NREC effort of the early 1960s that combined an attack simulator, an input-output model of the American economy, and logistics models of post-attack recovery, into a single program.



It is important to note that these models entailed a crucial shift in the object domain of catastrophe modeling and vulnerability mapping. The concern is no longer with the specter of a threatening enemy and a single nuclear detonation. Rather, it is with the *intrinsic* vulnerabilities of vital systems. Correspondingly, OEP began to focus on the concept of “survivable” systems – or, as they were increasingly called, “survivable networks” – such as oil pipelines and electricity grids. This interest in survivable networks was structurally similar to the concern with mitigating the vulnerabilities of communications systems that led, also during the late 1960s, to the development of the internet by ARPA; more research is needed to understand the links among these developments.

The role of operations research and systems analysis in these new system vulnerability models bears note. Much as statistics, on Foucault’s observation, provided a crucial knowledge-form for population security, systems analysis provided key technical instruments that made knowledge about the vulnerability of vital systems possible. As is well known, systems analysis was developed during and after WWII in relationship to military problems, such as building missile guidance systems or planning bombing runs. These were effectively optimization problems, in which the task was to maximize military “outputs”: kill rates or damage ratios, for example. In OEP and other contexts these techniques were redeployed. The scope of these models expanded, from relatively restricted technical problems concerning, for example, a weapons system, to a much broader understanding of the “system” or “network” that included much of the national economy of the United States, or at least important strategic sectors. And techniques of systems analysis – such as linear programming and Monte Carlo simulations – were used

not only for optimization problems but in analyses that focused on the *disruption* of vital systems. Effectively a shift had taken place, from an emphasis on the singularity of a nuclear attack to the inherent vulnerability of the U.S. economy's vital systems.

### **Generic Emergency**

So far we have looked at how concepts and techniques oriented to the security of vital systems emerged in the military context during the early-to-mid 20<sup>th</sup> century. We now want to trace their extension beyond this context, as vital systems security was “autonomized”, becoming in itself a goal of national security rather than just a part of military strategy. This process began within the Office of Emergency Preparedness in the late 1960s, and has gradually extended into other institutional arenas, including several recent initiatives in the Department of Homeland Security.

From its inception, OEP's mandate was not limited to nuclear war, but, as a 1962 Organizational Study put it, was concerned with “the development of planning assumptions and broad general objectives with respect to various conditions of national emergency” (p. 3). But in the early 1960s its focus was nonetheless firmly linked to the the problem of superpower conflict. By the mid- to late-1960s, however, OEP's reports and activities reflected a concern with the vulnerability of vital systems to a range of possible disruptions. Thus, the Preface to a 1968 report on the design of pipelines noted that “the United States is covered by a complex of networks for communication, transportation and the distribution of goods and energy. These networks not only play a vital role in the economy but are also critical factors in national security.” “The Office of Emergency Preparedness,” the Preface continued, “is an agency with responsibilities that

relate to the effects upon these networks of natural disaster or enemy attacks. To fulfill these responsibilities the OEP is required to have a thorough understanding of the analysis and design of such networks.”

By the late 1960s OEP had substantially broadened the scope of its activities to encompass a range of problems that involved “crises” and emergency response outside the context of war: natural disaster modeling, preparedness, and response; the management of economic crises, including strikes and economic shocks; and modeling energy crises. Thus, for example, OEP played a central role in hurricane response and recovery efforts beginning in the late 1960s. It also was the lead federal agency in organizing the wage-price freeze under U.S. President Richard Nixon in 1971, and produced reports on energy system vulnerability, conducting studies of pipeline security and of conservation measures that figured in a broader national discussion about energy security.

The critical point is that officials in OEP increasingly recognized that the tools, such as catastrophe modeling and vulnerability analysis, that they had developed in order to anticipate and prepare for nuclear war might be useful in dealing with a range of emergencies outside the traditional concerns of national security. The type of threats these tools focused on shared certain common characteristics. First, they were uncertain but potentially catastrophic events that could not be deterred or interdicted. Second, such potential emergencies could disrupt the country’s vital systems – the infrastructures, industrial systems, and economic mechanisms – upon which the U.S. polity and economy depended. Third, these events could be “managed” primarily by reducing the vulnerability of these systems and by developing generic response capacities.

What was underway during this period, we suggest, was a generalization of system-vulnerability thinking: that is, the application of its characteristic techniques, forms of reasoning, and practices beyond the context of nuclear war to a range of potential emergencies. This generalization also entailed a shift in the relationship between system-vulnerability and national security. Some of the new threats identified by OEP – economic shocks, energy crises, terrorist attacks – were indeed seen as problems of national security. But this was true in part because the concept of “national security” was itself in a process of significant extension and expansion. During the 1970s, issues other than superpower confrontation – such as energy and terrorism – were increasingly identified as national security problems. This is not to say that vital systems security was completely separated from military concerns. But in some sense vital systems security had become “unblocked” to become a more general framework that itself could serve to redefine what counted as national security problems.

We can illustrate how this process worked by examining two cases in which techniques initially associated with Cold War military preparedness were applied to objects traditionally associated with population security – creating an autonomous field of vital systems security. Each of these cases illustrates a key feature of vital systems security. First, its *object* of knowledge and intervention, the “vital system”. And second, its treatment of *events* – the imaginative enactment of uncertain, potentially catastrophic threats.

### **Infrastructure: From Population to Vital System**

Let us begin with a case of the “object” – namely, the vital system itself. Vital systems, as we have seen, are systems that are essential for the continued functioning of modern polities and economies, such as transport and energy networks, financial systems, health systems, and communication systems. Of course these systems are longstanding objects of population security, and were crucial to strategies of economic development and social welfare throughout the 20<sup>th</sup> century. What is general in such efforts is an emphasis on infrastructure construction, integration, and standardization, and an orientation to norms of reliability, productivity, and welfare. But beginning in the 1960s and 1970s, these systems were constituted as objects of knowledge and intervention in relation to an entirely different set of problems. These problems did not have to do with the absence of infrastructure, its fragmentation, or routine breakdowns – the traditional concerns of population security. Rather, they were linked to the very success of infrastructural modernization: the fact that collective life depended on complex, integrated infrastructural systems that were vulnerable to disruption.

To illustrate, let us take the example of energy infrastructures. The vulnerability of infrastructure systems to enemy attack – and in particular energy systems – had long been addressed in the context of civil defense and defense production planning. In the 1960s, OEP was using new tools of systems and network analysis to think about the complex patterns of disruption that a nuclear attack would have on oil and electricity infrastructures. Key figures in OEP clearly saw the organization’s mission as concerned broadly with the vulnerability of these vital systems. Thus, for example, in a 1969 report on “Critical Networks in a Post-Attack Environment,” Robert H. Kupperman, the head of the Systems Evaluation Division of OEP, wrote “During a nuclear attack on the United

States, many of the nation's large networks will be damaged. Most important are the transportation, energy distribution and communication systems. Energy distribution facilities include oil and gas pipelines as well as the electric power grid.” He argued that there was a “vital need to determine realistic planning factors concerning the economic impact of damaged networks and the capabilities for restoration,” suggesting that “network analysis provides a new method for both short and long range recovery plans.”

But soon these concerns about infrastructure vulnerability were focused by events other than nuclear war: terrorist attacks on the electricity grid, particularly by domestic groups; the oil shocks in the early and late 1970s; major blackouts in the United States; and catastrophic natural disasters such as Hurricane Agnes in 1972. For Kupperman and a group of like-minded national security thinkers, these events indicated that the nation’s dependence on critical systems was a vulnerability that could be exploited by enemies who lacked the military strength to directly challenge the U.S. But the same dependence on vital systems created vulnerabilities to other kinds of threats. Kupperman noted that disruptions such as the 1965 blackout “gave an indication of what would happen to portions of this country in case of a widespread power failure.”

Such arguments followed the concern, first developed in strategic bombing theory, with critical nodes of a production system that, if disrupted, could knock out an entire industrial web. There was a crucial difference, however. The threat now came not from an enemy’s military attack, but from non-deterrable threats – terrorism, and “threats without enemies” such as technological failures and natural disasters. In short, preparedness was no longer viewed as an adjunct to superpower confrontation. Rather, it was a security problem in its own right, one that was reflected in a range of discussions

through the 1970s. Concern about the infrastructure vulnerability was thus one important context in which vital systems thinking was de-coupled from military problems.

These concerns were reflected in a number of government reports throughout the period. For example, in 1977, the Joint Congressional Committee on Defense Production held hearings and published a two-part report on the nation's "civil preparedness" programs. The report criticized the nation's emergency management plans, and recommended a broadening of these efforts to include non-nuclear threats. The first volume of the report articulated, in now-familiar terms, two key aspects of the vital systems security framework: the dependence of contemporary society on complex technological systems, and the vulnerability of citizens to multiple types of threat: "An increasingly complex, technology-dependent, industrial economy in the United States," the report argued, "has made citizens more than ever vulnerable to the effects of disasters and emergencies over which they have little or no control and to which they cannot successfully respond as individuals" (United States. Joint Committee on Defense Production 1977, 3). Here the state's obligation to provide security to its citizens explicitly includes the demand to mitigate vulnerabilities to a wide variety of potential emergencies.

In July 1977, soon after the Committee's *Civil Preparedness Review* was published, a major blackout occurred in New York City. The blackout, which was accompanied by extensive riots and looting, brought widespread attention to the frailty and vulnerability of the nation's electrical grid and other critical systems. The Defense Production Committee held hearings shortly after the blackout on the implications of the event for federal emergency preparedness.

At these hearings, the Director of the Defense Logistics Agency testified about military efforts to protect key defense industries from attack. He noted that the scope of his agency's activity was limited to those industries that had a direct impact on defense needs. Considering the widespread impact of the New York City blackout on economic and social life, he suggested the need for a broader program to secure critical facilities. This would begin with a cataloguing effort: "It might be well if there were some sort of national list, if you please, of facilities that would be a key to our economic and societal well-being. Then at least, we would know what they are and whether or not the Federal Government would see fit to involve itself in providing for their security or would provide at least some advice on what these facilities could do for themselves" (United States. Joint Committee on Defense Production 1977, 117).

What is significant in these recommendations is the proposal that the Federal Government should generalize its efforts to assure critical infrastructure: from a specific emphasis on those systems essential to military production, to a broader concern with the vital systems essential to the economic and social well being of the nation as a whole. Broadly speaking, by the late 1970s the framework of contemporary Critical Infrastructure Protection initiatives had been established. It is visible in many contemporary initiatives, for example, a recent Presidential Report on Critical Infrastructure Protection which led to the "National Strategy for the Protection of Critical Infrastructures and Key Assets". In this strategy, the term "critical infrastructure" refers to technological systems for sustaining social and biological life, often initially developed as part of population security. Among the sectors included in the "National Infrastructure Protection Plan" are: agriculture and food, public health and healthcare, drinking water

and waste water treatment, energy, banking and finance, defense industrial base, telecommunications, chemical, transportation systems, and emergency services. Here are the basic elements of Critical Infrastructure Protection, which we can talk about later if there is interest.

### **Constituting the Event: Imaginative Enactment**

Let us now turn to another key feature of vital systems security – how it constitutes potential future *events* as objects of knowledge and intervention. It does so not through statistical analysis based on historical incidence, but rather through what we call practices of “enactment.” Specifically, we’ll look at one form of imaginative enactment, the scenario-based exercise. The scenario-based exercise is a classic sovereign state security technique – as is well known from the traditional “war game”. But increasingly, since the 1970s, it has been applied to “threats without enemies” such as terrorists, catastrophic disease or large-scale natural disasters.

First: how are scenarios used within sovereign state security? From this vantage, they are part of military strategy: they help in understanding and intervening in the actions of foreign adversaries. Thus Cold War scenario-based exercises involved simulated conflicts between a “red team” (representing the Soviet Union) and a “blue team” (the US). The goal of such exercises was for officials to envision the likely behavior of the enemy in a diplomatic or military crisis and to learn in advance how to respond strategically.

However: once events other than military confrontation are taken up as national security problems, we see the use of scenario-based exercises without a red team as an

opponent – rather, it is used to generate knowledge about internal system vulnerabilities. This can be seen in the use of scenarios by the Department of Homeland Security. Formed in the wake of 9/11, DHS is often thought of as a counter-terrorism agency – but it is perhaps better understood as a collection of multiple agencies with diverse missions: counter-terrorism, disaster response, border security, etc. Critically, it includes FEMA, the federal emergency response agency that was itself an extension of the civil defense establishment. One issue DHS is faced with is: how to deal with an array of potential threats that cannot necessarily be prevented or deterred but whose consequences might be catastrophic? Here DHS has adopted and extended Cold War planning techniques – focusing not on a foreign enemy but on a “generic” emergency.

In its recent planning documents, DHS has outlined a broad strategic rationale of what it calls “national preparedness.” Its *National Preparedness Guidance* elaborates a set of administrative mechanisms for making preparedness a measurable condition. The plan is a guide for decision-making and self-assessment across multiple governmental and non-governmental entities concerned with problems of domestic security. It seeks to bring disparate forms of threat into a common security field.

What is key to this normative rationality is that the threat DHS must address is conceptualized not in terms of a foreign enemy’s capabilities and intentions, but in terms of the nation’s own vulnerabilities and response capacities. So, how does it make this kind of calculation? Here is where scenario-based planning proves useful. DHS selected 15 disaster scenarios as “the foundation for a risk-based approach.” These scenarios are not predictions or forecasts: rather, they map readiness for a wide range of threats. These potential events – including an anthrax attack, a flu pandemic, a nuclear

detonation, and a major earthquake – were chosen on the basis of plausibility and catastrophic scale. Again, these events differ both from traditional sovereign state security threats in that they are difficult or perhaps impossible to deter, and they are unlike traditional population security threats in that there is no archival record of their occurrence on which one could base risk evaluations.

As an alternative, the DHS scenarios make it possible to generate knowledge of current vulnerabilities and the capabilities needed to mitigate them. Using the scenarios, DHS has developed a menu of the “critical tasks” that would have to be performed in various kinds of major events; these tasks, in turn, are to be assigned to specific governmental and nongovernmental agencies. It is through the technique of imaginative enactment, then, that diverse and unpredictable events are brought into an apparatus of preparedness.

Thus, the goal of DHS preparedness planning is to “attain the optimal state of preparedness.” As the plan defines this state: “Preparedness is a continuous process involving efforts at all levels of government and between government and private-sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required resources.” In other words, preparedness is the measurable relation of capabilities to vulnerabilities, given a selected range of threats. Scenarios make it possible to do “Capabilities-based planning”:

“[Capabilities-based planning] addresses the growing uncertainty in the threat environment... Target levels of capability will balance the potential threat and magnitude of terrorist attacks, major disasters, and other emergencies, with the resources required to prevent, respond to, and recover from them.”

## **Conclusion**

In conclusion, let us quickly summarize our argument: first, we traced part of the genealogy of a new technology of power, vital systems security - focusing especially on the role of developments in the conduct of war as they have been extended into new domains. Second, we showed a couple of features of how vital systems security works through two cases, energy infrastructure and homeland security scenarios: it is distinctive from prior forms of security in its object of knowledge and intervention, and in its treatment of potential future events.

The identification of vital systems security is significant, we think, not only in the context of recent national security initiatives in the US and in other countries, but also internationally – one can see its elements in current approaches to a number of global “threats without enemies”: including “resilience” based approaches to climate change; or “preparedness” based methods for dealing with humanitarian emergencies. Arguably – and this is a point we would be glad to take up in discussion – the techniques of vital systems security prove especially useful in non-state settings in which the implementation of population security measures – such as poverty reduction or public health – proves impractical, whether for technical or political reasons. Indeed, we would suggest that the next step in a research program on vital systems security would be to investigate precisely these points of articulation – and disarticulation – between sovereign state security, population security and vital systems security.