Public Interest Report

THE FEDERATION OF AMERICAN SCIENTISTS VOLUME 63, Number 3 Fall 2010

Systems Resilience and Nonproliferation

Arian Pregenzer of Sandia National Laboratories writes about the growing concerns about the resilience of the nuclear nonproliferation regime.

Read more on page 3.

Non-State Actor Nuclear Command & Control

FAS's Charles Blair, director of the new Terrorism Analysis Project, provides an explanation of paradigms that have emerged since the conclusion of the Cold War.

Read more on page 9.

Cyber Warfare: Surviving an Attack

Created to minimize the vulnerability of United States communications networks to a crippling nuclear first strike by the Soviet Union, the Internet is turning into a battlefield.

Read more on page 14.

About FAS

The Federation of American Scientists (FAS), founded in 1945 as the Federation of Atomic Scientists by Manhattan Project Scientists, works to ensure that advances in science are used to build a secure, rewarding, environmentally sustainable future for all people by conducting research and advocacy on science public policy issues. FAS is a tax-exempt, tax deductible 501(c)3 organization.

FAS

Public Interest Report

Fall 2010, Volume 63, Number 3

ADDRESS SERVICE REQUESTED

FAS Public Interest Report
USPS No. 188-100
is published quarterly at:

1725 DeSales Street, NW
6th Floor
Washington, DC 20036

Periodicals postage paid at
Washington, DC

POSTMASTER:
SEND ADDRESS CHANGES TO

FAS Public Interest Report
1725 DeSales Street, NW
6th Floor
Washington, DC 20036

Annual Subscription is $50/year.
Copyright 2010 by the Federation of American Scientists.

Archived FAS Public Interest Reports are available online at ww.fas.org.

Phone: 202.546.3300
FAX: 202.675.1010
Email: fas@fas.org

EDITORIAL STAFF
Editor: Charles D. Ferguson
Managing Editor: Monica Amarelo

PRESIDENT'S MESSAGE

Innovative Thinking:

Challenging Conventional Wisdom

I am pleased to announce a new look for the PIR. Beginning with this issue, the PIR offers expanded coverage in new issue areas such as terrorism analysis and cyber security.

As you will notice from the bylines, not all of the authors are FAS staff. In particular, Arian Pregenzer is a senior scientist from Sandia National Laboratories, and Devabhaktuni Srikrishna is an information technology expert and was the founder and Chief Technology Officer of Tropos Networks. In future issues, the editorial staff will include more outside FAS staff as authors.

You will also notice that this issue is longer than most of the past issues. It is about 50 percent longer. This is due to saving costs through electronic publishing. FAS members and PIR subscribers thus gain twofold: a greatly expanded PIR and faster delivery. Instead of having to wait for the snail mail delivery, members and subscribers will receive—starting with this issue—the PIR one full week in advance of anyone else.

For those non-members who are reading this issue, I encourage you to become a member, be one of the first to get the innovative thinking in the PIR, and help support FAS in its work to make the world more secure.

These innovative publication changes complement the stimulating analysis in this issue. Dr. Pregenzer applies principles from ecology to challenge our thinking about how to prevent the further spread of nuclear weapons. Charles Blair's article shakes up the conventional view about what terrorists would do if they acquired nuclear weapons. Mr. Srikrishna examines many of the complexities of cyber warfare. Lindsey Marburger's article describes a new FAS initiative called the International Science Partnership, which aims to bring together U.S. scientists and engineers with their counterparts in the developing world. The article discusses, in particular, the start of this initiative's pilot project in Yemen and the urgent water management and related security problems there.

And finally, the issue discusses a new FAS program called Students for International Security designed for undergraduate and graduate students interested in doing their part to work toward a more secure world.

I hope you feel smarter after reading this issue. If you have any comments or questions, please let the editors know. **FAS**

Systems Resilience and Nuclear Nonproliferation

By Arian Pregenzer, Senior Scientist in the Global Security Program at Sandia National Laboratories, Albuquerque, NM.

Introduction

There are growing concerns about the resilience of the nuclear nonproliferation regime. Some fear that we are reaching a nuclear "tipping point" and predict a cascade of proliferation in the Middle East if Iran is successful in acquiring nuclear weapons; some caution that Japan could reverse its long-held commitment to nonproliferation in the face of the North Korean threat and a rising China.

Underlying these concerns is a sense that global commitment to the nonproliferation regime is waning. Whereas the United States has elevated nuclear proliferation to the top of its list of national security threats and is working vigorously to prevent Iran from acquiring nuclear weapons, many countries see nonproliferation as primarily a U.S. issue, and some view U.S. military superiority as the greatest threat to their security and resist pressure to follow the U.S. lead in treating nonproliferation as the highest priority.

The goal of this paper is to introduce the concept of systems resilience as a new framework for thinking about the future of the nonproliferation regime. First, I define the terms "complex system" and "resilience" and make the case that the nonproliferation regime is a complex system. Next, I discuss key themes from the literature on systems resilience and apply them to the nonproliferation system. Based on this discussion, I suggest that the resilience of the nonproliferation system can be increased by acknowledging that determined states cannot be prevented from acquiring nuclear weapons and instead focusing on 1) developing new international capabilities to respond to proliferation, 2) reducing resources expended on outdated strategies, and 3) increasing the diversity of the champions of the nonproliferation regime.

Definitions

A complex system is a dynamic network of many interconnected elements, in which changes in some elements (or the relations among them) produce changes elsewhere. In addition, the properties of the system as a whole are different from the properties of its individual elements. This is referred to as "emergent" behavior. It is difficult to predict, control, or understand the effects of actions in a complex system, especially when its elements are tightly connected and disturbances propagate easily. Actions always have unintended consequences, as positive and negative feedbacks among system elements cannot be known in advance. Coherent behavior, if it occurs, arises from competition and cooperation among the system elements, and results from very large numbers of individual actions. Order is emergent, rather than pre-determined. [1]

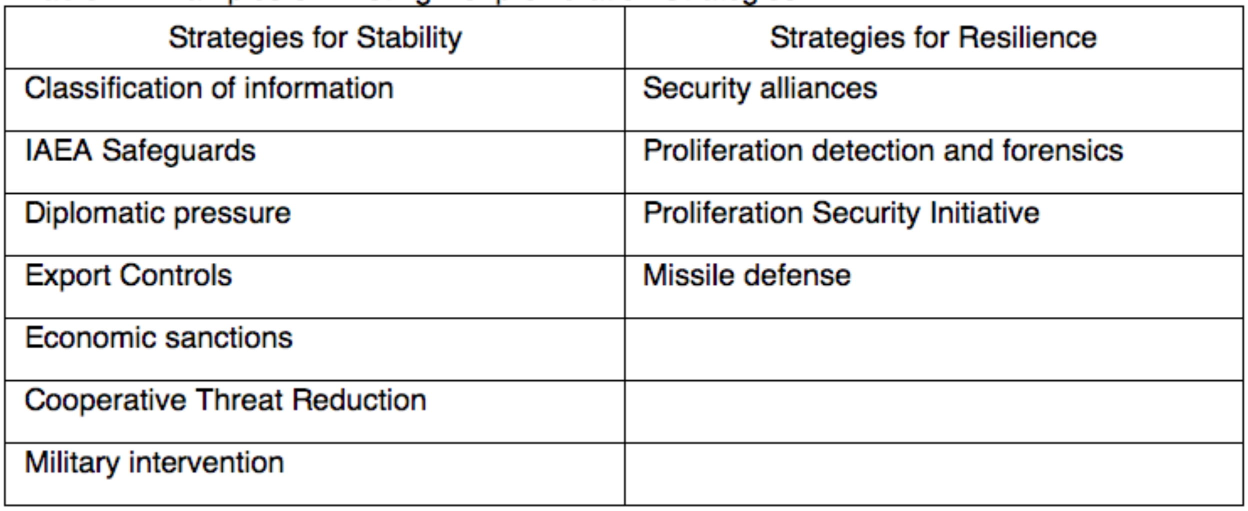
Resilience is a measure of a system's ability to absorb continuous and unpredictable change and still maintain its vital functions. After a significant disturbance, some of the system's elements might change, or be related to each other in different ways, but if the system can adapt sufficiently so that it continues to perform its vital functions, it is resilient. In contrast to resilience, stability is a measure of a system's ability to resist change and to bounce back to its original configuration after a perturbation.

The concept of systems resilience has been explored extensively in the last twenty years in the context of social-ecological system sustainability. [2] Three themes are particularly relevant to a discussion of the nonproliferation regime: 1) the difference between resilience and stability, 2) the need for evolution to maintain function in a changing environment, and 3) the importance of functional and demographic diversity.

The Nonproliferation System

The set of actors, institutions, and strategies aimed at preventing the spread of nuclear weapons can be thought of as a complex system whose emergent property is a strong international norm against nuclear proliferation. Different actors have

Table 1: Examples of Existing Nonproliferation Strategies



Strategies for Stability	Strategies for Resilience
Classification of information	Security alliances
IAEA Safeguards	Proliferation detection and forensics
Diplomatic pressure	Proliferation Security Initiative
Export Controls	Missile defense
Economic sanctions	
Cooperative Threat Reduction	
Military intervention	

different priorities, making it difficult to predict the impact of nonproliferation strategies in advance. For example, controlling the supply of sensitive nuclear technology raises the threshold for acquiring nuclear weapons, but it can also make such technology more desirable and increase demand, which could stimulate establishment of illicit supply networks, which are more difficult to detect and control. Military intervention to end a nascent nuclear program may act as a powerful deterrent to some states considering clandestine programs; on the other hand, it may be seen as misuse of military power by others and undermine their commitment to implementing nonproliferation norms.

Despite these complexities, decades of embracing the Nuclear Nonproliferation Treaty (NPT) and engaging in nonproliferation practices (e.g., placing civilian nuclear material under International Atomic Energy Agency (IAEA) safeguards, controlling exports, and protecting nuclear material and weapons) have created a strong international norm against the spread of nuclear weapons. Although its strength is difficult to measure, I suggest that maintaining this international norm is the most important function of the nonproliferation system.

Difference between Resilience and Stability

Strategies to promote system resilience will be fundamentally different than strategies to promote stability. Strategies for stability will emphasize avoiding danger and controlling both system elements and the external environment. They will focus on detailed plans to prevent a broad range of hypothetical threats. Strategies for resilience will acknowledge the inevitability of change and focus on establishing general capabilities to respond to unknown hazards as they occur. Rather than avoiding danger, strategies for resilience will use an experimental approach to probe the environment: stressing the system to strengthen it. [3]

Most existing nonproliferation strategies can be classified as strategies for stability. Controls on the supply of nuclear weapons-relevant material, technology and expertise are explicitly designed to prevent additional states and non-state actors from acquiring the means to make nuclear weapons. International Atomic Energy Agency (IAEA) safeguards are intended to prevent diversion of nuclear material from civilian to military use; cooperative efforts to secure nuclear weapons and material are aimed at preventing unauthorized access or illicit transfer across and within national borders. Diplomatic strategies and sanctions seek to control the environment by offering potential proliferants a combination of carrots and sticks to dissuade them from nuclear ambitions. Military intervention has been used only occasionally, but again the aim has been to prevent or delay acquisition of capabilities to produce nuclear weapons.

Relatively little attention has been devoted to reducing motivation to acquire nuclear weapons in the first place or to developing broad international capabilities to respond to proliferation when it occurs. Security alliances address a broad range of security objectives and one outcome has been reduced motivation for states included in the alliances to develop their own nuclear weapons. There are also a number of strategies designed to provide early warning of proliferation and to enhance international response capabilities: the IAEA Additional Protocol would improve the IAEA's ability to detect clandestine nuclear activities and the Proliferation Security Initiative (PSI) aims to detect and interdict illicit shipments of proliferation-relevant material or technology. Other efforts to improve international nuclear detection and forensics capabilities are also underway. [4] Ballistic missile defense is yet another strategy to enable response, even though it has not received wide international support and most current systems are aimed at specific threats, such as Iran and the DPRK.

The Need for Evolution to Maintain Function

Systems must continuously evolve to maintain their performance in a changing environment, much less to improve. Evolution includes two types of change: strengthening existing capabilities and developing new ones.

The current nonproliferation system has evolved in both ways over the years in response to a changing international environment. After the failure of the Baruch Plan to win international support in 1946, the primary U.S. nonproliferation strategy was classification of information related to the nuclear fuel cycle and nuclear weapons. When Soviet and British nuclear weapons tests in the late 1940s and early 1950s demonstrated weaknesses of this approach, classification guidelines were modified, but not abandoned. The IAEA was created to promote nuclear power for peaceful purposes and also to safeguard civilian nuclear material. IAEA safeguards coupled with diplomacy (mostly bilateral) were the prevailing nonproliferation strategies until the Indian nuclear test in 1974, which triggered much more intensive efforts on international export control and the formation of the Nuclear Suppliers Group. The end of the Soviet Union in 1991 and fears of unsecured nuclear weapons and material was a significant shock to the nonproliferation system and resulted in creation of a broad range of cooperative threat reduction efforts to improve nuclear security; in the same time frame, the failure of the IAEA to detect the Iraqi nuclear program led to the IAEA Additional Protocol.

Since the shock of 9/11 and revelations about the A.Q. Khan black-market raised the specter of nuclear terrorism, many fundamentally new approaches have been tried, ranging from capacity building to help developing countries implement nonproliferation obligations, to the Proliferation Security Initiative aimed at interdicting illicit shipments, to limited ballistic missile defense, to preemptive war in Iraq. The Obama administration has recently embraced yet another strategy: reducing the salience (and numbers) of nuclear weapons to demonstrate U.S. commitment to NPT Article VI and to increase support by nonnuclear weapon states for implementation of stronger nonproliferation measures.

The Importance of Diversity

Diversity is essential for resilience. For example, the resilience of ecological systems is enhanced if different organisms performing the same ecological function respond differently to environmental perturbations, thereby enhancing the likelihood that the service will be maintained throughout a wide range of conditions. [5] Loss of diversity increases the chances for ecosystem collapse. In the business world, diversity in workplace skills, personalities, and perspectives is believed to enhance creativity and innovation and to improve decision-making and problem-solving, leading to better products. A demographically diverse workforce also may have a better understanding of the demographics of the marketplace, enhancing its competitive edge.

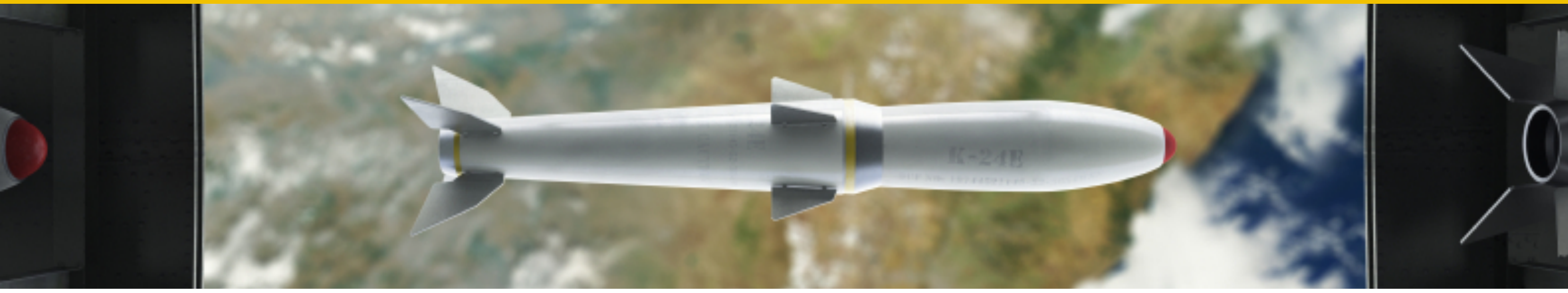
> *"Systems must continuously evolve to maintain their performance in a changing environment, much less to improve. Evolution includes two types of change: strengthening existing capabilities and developing new ones."*

How diverse are the strategies, institutions, and actors of the nonproliferation system? The previous discussion suggests that the current set of nonproliferation strategies lacks diversity, as most are focused on controlling supply. Traditional nonproliferation institutions, such as the IAEA and the NSG, also focus primarily on controlling supply, although the IAEA also plays an important role in facilitating international cooperation on civilian nuclear technology. New strategies and institutions are emerging, however, that could increase diversity. For example, the PSI focuses on detection and interdiction through a "coalition of the willing" rather than through a traditional (bureaucratized) international institution.

The greatest diversity of the nonproliferation system lies in its actors, in terms of both their motivations and the roles they play. Indeed, broad international support for the nonproliferation system emerges from a diverse set of motivations: some actors emphasize that security for all states is increased by limiting the spread of nuclear weapons, others support nonproliferation as a means to the elimination of nuclear weapons world-wide, some are primarily interested in maintaining existing international balance of power, yet others emphasize access to peaceful nuclear technology.

Actors in the nonproliferation system also play a number of different roles: there are the champions, the (sometimes ambivalent) participants, and the challengers. Western states and their allies are the most vocal champions of nonproliferation, with the United States the most prominent. Champions among the nonnuclear weapon states generally have advanced civilian nuclear industries and many possess the technological capability to develop nuclear weapons should they desire. Although this group is fairly uniform from the perspective of economic development, they do not all agree about nonproliferation strategies. For example, Canada and Australia both objected to U.S. attempts to restrict further acquisition of uranium enrichment capabilities because it would have limited their options as uranium suppliers; South Korea wants to develop spent fuel reprocessing capabilities in spite of U.S. objections.

There are also many states, both with and without nuclear weapons, who participate in the nonproliferation system with varying degrees of commitment. For example, China and Russia are active participants, but see U.S. "hegemony" as a greater threat to their security than nuclear proliferation. Some, such as Brazil and Argentina focus primarily on the rights of nonnuclear weapon states to the full range of nuclear technology and resist additional nonproliferation requirements, such as the IAEA Additional Protocol.



Others, such as South Africa and Egypt, emphasize the importance of NPT Article VI and consistently press nuclear weapon states to disarm. This is highly diverse group geographically, economically and politically.

Finally, there are the challengers of the current regime: states that openly defy international norms, such as North Korea, and states that are widely believed to aspire to nuclear weapons clandestinely, such as Iran.

The Adaptive Cycle

The concept of an adaptive cycle has been developed to inform discussions of resilience in ecological systems. [6] According to this concept, resilient systems do not tend toward a stable equilibrium. Rather, they pass through characteristic phases associated with growth, conservation, release, and reorganization. The growth phase is characterized by great innovation and experimentation. As the system matures innovation and experimentation slow and it enters the conservation phase, which is characterized by specialization and high connectivity among all system elements. High connectivity and specialization increase efficiency, but at the expense of flexibility, and the system's ability to respond to disturbance decreases. Eventually a perturbation arrives that stresses the system past its breaking point, and triggers system collapse (or release), whereupon significant changes in system elements and their relationship to each other may occur. The release phase is followed by a period of reorganization during which new ideas, policies, or species can arise. The cycle then repeats itself. A resilient system can maintain its function over time as it passes through one or more cycles. In contrast, a non-resilient system, such as a sand-pile accumulating more and more sand until it finally collapses, cannot recover.

Looking at the nonproliferation system through the lens of the adaptive cycle, which phase is it in? An argument could be made that it is in the conservation phase and therefore particularly vulnerable to major shocks: The cumulative evolution of the nonproliferation system has resulted in an inflexible and overburdened system that is incapable of responding to the challenges ahead, challenges that certainly will require greater agility and innovation.

On the other hand, an argument could be made that the system is in the early stages of a growth phase: Although attempts to change the existing system after the shocks of 2001 have had limited success, experimentation with new approaches falling outside the traditional structure of the nonproliferation regime is vigorous and ongoing. Lessons from these experimental efforts will be taken into account as new ideas evolve.

Reality is most likely a combination of both: Although many innovative ideas are now being tried, the old approaches remain and continue to burden the system. In addition, the impact of many of the newer approaches remains unknown and international support remains uncertain. The critical question is how to increase the resilience of the nonproliferation system in this transitional period.

New Approaches to Enhance Resilience

The discussion in the preceding sections suggests several inter-related themes to guide development of more resilient approaches: 1) experiment with new ideas to enhance resilience rather than continue to focus on strategies for stability; 2) reduce or eliminate resources expended on outdated strategies that contribute little to stability or to prevention; and 3) increase the diversity of nonproliferation champions. If systems resilience is a useful framework for analyzing nonproliferation, much more work would need to be done to develop new approaches. The following ideas are intended to stimulate discussion.

Experiment with New Approaches

Strategies emphasizing resilience will focus on developing general capabilities to respond to proliferation, acknowledging that determined states cannot be prevented from acquiring nuclear weapons. The effort to develop reliable, versatile missile defense is an example. However, to contribute to the resilience of the international nonproliferation system, missile defense must not be perceived as furthering the interests of just a small subset of nonproliferation actors which is how it is often characterized today. Understanding potential unintended consequences of missile defense (such as alienating China and Russia) and taking steps to reduce them will be essential to its making a positive contribution to the international nonproliferation system.

Establishing new multilateral security structures that serve a broad set of needs, but also undertake proliferation-relevant missions such as response to nuclear events and defense against the threat of nuclear use, could be explored. Exercises, such as those conducted under the auspices of the PSI, would play a critical role. Precedents exist for such security structures, such as the Cooperative Defense Initiative (CDI) that brings the United States, the Gulf Cooperation Council, Egypt and Jordan together for military coordination purposes. International Peace-Keeping

also might provide useful lessons learned.

General response capabilities have value even if proliferation never occurs. Missile defense can be used against conventional threats, and new security structures can be used to resolve regional conflicts over a broad range of issues, such as disputes over territory and natural resources. In addition, the ability to respond effectively to proliferation might reduce states motivation to invest in nuclear weapons programs, if they knew in advance that their military value would be limited. [7]

Reduce Resources Expended on Outdated Strategies

Nonproliferation strategies have evolved largely through a cumulative process: new strategies are added but older strategies remain. For example, export control and classification of information continue to absorb enormous resources, even as technology and information have become widely available in the public domain. Expending the majority of IAEA inspection resources on safeguarding Japan's civilian nuclear infrastructure because of outdated rules about allocation of resources is another case in point.

This cumulative process has a huge opportunity cost, which inhibits exploration and development of the new approaches that have arisen in the last decade. Although it would be unwise to completely eliminate classification of nuclear weapons information and export controls, these approaches need to be brought up to date with the reality of global availability of technology and information. Refocusing efforts on protecting what is absolutely essential will free up resources that could be used more productively elsewhere. [8]

Similarly, with the expansion of nuclear energy globally, allocation of the majority of IAEA resources to inspect proliferation champions such as Japan makes little sense. Technologies such as remote monitoring can free up human resources, but new procedures for allocating resources must be developed to maintain relevance.

Increase the Diversity of Nonproliferation Champions

Paradoxically, attempts by the United States to heighten world-wide awareness of the dangers of nuclear terrorism and proliferation, coupled with unilateralist approaches, have created an impression that nonproliferation is a U.S. issue and that taking it seriously is tantamount to giving in to U.S. demands. Although the current administration has embraced multilateralism, it has named nuclear proliferation and terrorism as the top two threats to U.S. security. This may only reinforce the perception in some countries that nonproliferation is a proxy for U.S. hegemony.

To counter this perception, the potential reactions of nonproliferation champions and ambivalent participants must be considered explicitly when making decisions about nonproliferation strategies. The diversity of motivations among the supporters of nonproliferation strengthens the system and should be maintained, even though it also introduces tension about policies and priorities. New strategies are needed that explicitly take this diversity into account. Recent commitments by the United States to reduce the numbers and salience of nuclear weapons is an example of a strategy aimed at increasing support for nonproliferation by key "ambivalent" states, although its impact is not yet clear.

Another example concerns the approach to the spread of sensitive nuclear technology. Rather than publicly seeking commitments by others not to pursue enrichment and reprocessing capabilities, states with the greatest stake in nonproliferation could lead by example and establish multinational enrichment and spent fuel reprocessing facilities. Political resources could be directed to overcoming domestic resistance to controversial new approaches, such as spent fuel take back. Commitments with individual states not to develop sensitive nuclear technologies could still be pursued privately as part of establishing nuclear cooperation agreements.

The use of high-volume public pressure to convince countries such as Iran to give up nuclear weapons programs should also be reconsidered. Its primary result seems to be to increase domestic support for nuclear weapons programs in the face of threatening international rhetoric. Better results might be obtained by taking this debate out of the public eye and pressuring countries in private forums.

Final Thought

Although many worry about the repercussions of a nuclear capable Iran or developments in the North Korean nuclear program, it is impossible to predict the nature or timing of the next major challenge to the nonproliferation regime. In the past, some shocks have indeed come from events directly related to proliferation, such as the Soviet and Indian nuclear tests. However, the most resounding shocks to the nonproliferation regime have emerged from the wider external environment, namely the dissolution of the Soviet Union and the September 11 terrorist attacks. Acknowledging both the inevitability and unpredictability of future shocks, and relaxing the urge for control may be the most important steps to foster a climate for continued innovation that will underpin any ultimately resilient system. **FAS**

ENDNOTES

1. Three books have informed much of the discussion of complex systems in this paper: For discussions of complex systems, see Robert Jervis, *Systems Effects: Complexity in Political and Social Life* (Princeton, NJ: Princeton University Press, 1997); Aaron Wildavsky, *Searching for Safety* (Piscataway, NJ: Transaction Publishers, 1988); and Per Bak, *How Nature Works* (New York, NY: Copernicus Press, 1996)
2. For a good overview see Brian Walker and David Salt, *Resilience Thinking* (Washington, DC: Island Press, 2006). For an example of the application of the concept of resilience to homeland security, see Stephen Flynn, *The Edge of Disaster: Rebuilding a Resilient Nation* (New York, NY: Random House, 2007).
3. The ecologist C.S. Holling was among the first to articulate the difference between resilience and stability in his classic paper "Resilience and Stability of Ecological Systems," Annual Review of Ecological Systems, 1973, 4: 1-23. In addition, Aaron Wildavsky devotes much of his book *Searching for Safety* to the difference between strategies for resilience and strategies for prevention.
4. For example, see Jacob Goodwin, GSN: Global Security News, "DNDO wants to develop a "global nuclear detection architecture"" July 14, 2010: <http://www.gsnmagazine.com/article/21061/dndo_wants_develop_%E2%80%9Cglobal_nuclear_detection_archi
5. For a good discussion of the importance of diversity to resilience, illustrated with the example of Caribbean coral reefs, see Brian Walker and David Salt, *Resilience Thinking* (Washington, DC: Island Press, 2006), pp. 64 – 73.
6. This concept is developed through a series of articles and case studies in L. H. Gunderson and C. S. Holling, eds. *Panarchy: Understanding Transformations in Human and Natural Systems* (Washington, DC: Island Press, 2002). There is also a good non-technical overview in Brian Walker and David Salt, *Resilience Thinking* (Washington, DC: Island Press, 2006), pp. 74 – 95.
7. This argument mirrors that of Stephen Flynn in *The Edge of Disaster*, where he argues that rather than invest the majority of counter-terrorism resources in preventing terrorism, the United States would be better off, for example, by investing more resources to strengthen aging infrastructure. Not only would this enhance the foundations of economic security and improving resilience to natural disasters, it would also make it a less attractive target for terrorists and reduce their motivation to attack.
8. Note that the Obama administration has recently announced that it has launched a major review of the U.S. export control system, and aims to modify both the policy for determining what commodities and technologies are subject to controls and how the federal bureaucracy will apply the new policy and operate the system. See, for example, Baker Spring, Obama's Ambitious Export Control Reform Plan, The Heritage Foundation, September 20, 2010. http://www.heritage.org/research/reports/2010/09/the-obama-administrations-ambitious-export-control-reform-plan

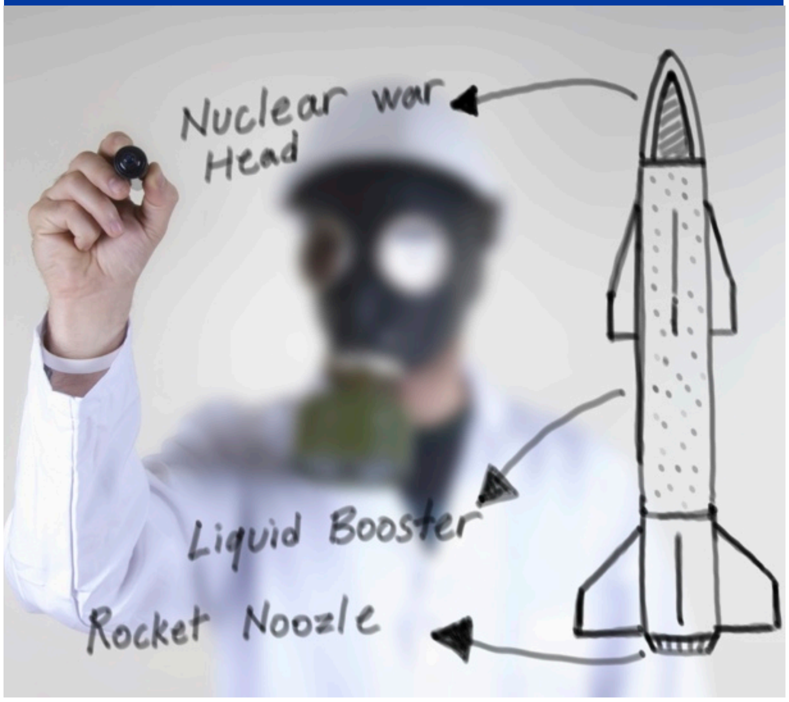
Arian Pregenzer is a Senior Scientist in the Global Security Program at Sandia National Laboratories, Albuquerque, New Mexico. Sandia National Laboratories is a multiprogram laboratory operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

"The most resounding shocks to the nonproliferation regime have emerged from the wider external environment, namely the dissolution of the Soviet Union and the September 11 terrorist attacks."

Non-State Actor Nuclear Command & Control

By Charles P. Blair, Terrorism Analysis Project, Federation of American Scientists

> *“ In contrast to Cold War parallels, alarmingly little attention has been given to how violent non-state actors would command and control a single nuclear weapon (or a nascent nuclear arsenal) or what their likely nuclear weapons employment policies (NUWEPs) would be.”*



Since the advent of mass-casualty terrorism, along with concomitant concerns over the use of chemical, biological, radiological, and nuclear (CBRN) weapons to achieve such ends, two parallels with Cold War nuclear paradigms have emerged. First, the United States is revisiting Cold War issues of civil defense and post-attack Continuity of Government (CoG) in preparation for actual terrorist employment of nuclear weapons on U.S. soil. [1] Second, there has been renewed scholarship—amid much speculation—about the technical obstacles violent non-state actors (VNSAs) face in attempting to fabricate improvised nuclear devices (INDs), capability and opportunity requirements for procurement of “off the shelf” nuclear weapons, and the likelihood and location of a domestic nuclear event. [2]

In contrast to these Cold War parallels, alarmingly little attention has been given to how VNSAs would command and control a single nuclear weapon (or a nascent nuclear arsenal) or what their likely nuclear weapons employment policies (NUWEPs) would be. [3] By limiting themselves to investigating only the general requirements necessary to attain a nuclear capability, contemporary scholars and analysts of the nexus between VNSAs and nuclear weapons bolster misguided assumptions that the *capability* to fabricate or obtain nuclear weapons tells us something about the manner of *employment* of that weapon. In short, most present perceptions of the possible marriage between VNSAs hostile to the United States and nuclear weapons foresee an immediate effort to use such devices against population centers within the United States, its territories or interests abroad, or its allies. Such a myopic view ignores the very real possibility that nuclear-armed

VNSAs could use pragmatic, cogent, and highly effective NUWEPs backed-up by complex and effective nuclear command and control structures.

Should the United States find itself facing such a nuclear-armed non-state adversary, the ability to successfully deter, prevent, preempt, react, or retaliate to a nuclear attack would be influenced by an understanding of that group's own perceived value of nuclear weapons and the arrangements the group has made to ensure that the weapon's perceived utility is maintained before, during, and after confronting its opponent. [4] Unfortunately, contemporary nuclear command and control paradigms either reflect Cold War assumptions or, with regard to VNSAs, presuppose dangerously narrow perceptions of the utility of nuclear weapons, custodial and employment options and targeting predilections.

The Potential Hazards of Enemy Decapitation: Authoritative and Delegative Command and Control Systems

The most troubling limitation to these antiquated and incompatible models lies in their inability to assess accurately if a given VNSA will employ, with regard to nuclear weapons, an *authoritative* or a *delegative* command and control system. [5] The former—where the decision to employ nuclear weapons is retained solely by a top leader(s)—allows the United States "decapitation" options against leadership centers to prevent or respond to an attack.[6] In contrast, a delegative system— an arrangement in which subordinate commanders are authorized to make nuclear employment decisions under certain defined circumstances—occludes decapitation opportunities; attempts to destroy a terrorist group's top-leadership, even if successful, might trigger the nuclear attack they were intended to neutralize.[7] In short, in the lead-up to a preemptive strike on a nuclear-armed VNSA or in the immediate aftermath of an attempted or successful nuclear strike on the United States or its interests, U.S. leadership's calculations about the authoritative or delegative nuclear command and control system employed by VNSAs will be of cardinal importance.

Command & Control Clues Found in Social and Organizational Psychology

Accordingly, the Terrorism Analysis Project of the Federation of American Scientists (FAS) is engaged in an eighteen-month study focusing on how VNSAs will approach and solve the challenges inherent in nuclear command and control.[8] There is no doubt that procurement by terrorists of a nuclear weapon would be a revolutionary occurrence; however, it may be possible to predict—and influence—variables that affect how the drama might unfold. As J. Robert Oppenheimer recalled just months after the nuclear bombings of Hiroshima and Nagasaki, "Nothing can be effectively revolutionary that is not deeply rooted in human experience." [9] Indeed, significant methodological elements of FAS's study—"Non-State Actor Nuclear Command & Control" — investigate established command and control paradigms.

First, for example, findings in social and organizational psychology may reveal important clues about the universal variables inherent in how dominion and delegation are balanced in complex and critical human interactions. The organizational cultural model created by the influential organizational psychologist Edgar Schein dictates that outsider discernment of the true nature of an organization— its resolution of the problem of external adaptation and internal integration (e.g., how a VNSA might construe nuclear command and control)—is not possible through examination of its visible behavior, its statements or its creed. [10] Similarly, fundamental elements of the organization's identity are not accessible with an understanding of its stated values and attitudes. Rather, according to Schein, the underlying and driving elements that determine the organization's identity are determined largely by a group's tacit assumptions—the unseen elements of a group's culture that are often unspoken. In short, some branches of organizational and leadership studies imply, the best way to predict the types of complex and novel interactions inherent in a VNSA's nuclear command and control is to go beyond the clues offered by cultural artifacts and its professed organizational nature; true organizational apprehension is only possible through an understanding of unstated, often taboo, assumed rules and "norms" of behavior.

State Nuclear Command & Control Paradigms

In contrast to the value of endogenously constructed cultural and organizational norms implied by organizational and social psychology, vis-à-vis their utility in unraveling potential VNSA command and control structures, a second methodological approach of FAS's study involves more traditional investigations of *state* nuclear management arrangements—partially exogenous

variables. Useful open source investigations exist about the variables likely to influence a state's perception of optimal nuclear command and control structures.[11] Peter Feaver, for example, suggests that the greater the "time urgency"—e.g., how quickly an arsenal must be made ready for rapid and immediate use— the more likely the command and control system will be delegative.[12] Some key factors in this regard are the size of the state's arsenal and its proximity to the threat, risk of high precision weapons in the enemy's arsenal (leading to increasing odds of decapitation), and *inter alia* lack of "geographic depth" in which to situate an arsenal. [13] Such physical circumstances might drastically reduce deployment options exposing the few available locations to enemy surveillance. By exploring the similarities and differences between state nuclear command and control and other variables believed to play a potential role in VNSA nuclear management arrangements, it may be possible to discern if certain variables, akin to "time urgency," are "structural"—if they are inescapably inherent to the issue of nuclear command and control and *must* be confronted by nuclear-armed VNSAs regardless of their internal qualities (e.g., organizational culture) or past behavior. [14]

Terrorists and Previously Displayed Command & Control Arrangements

FAS's Non-State Actor Nuclear Command & Control study also investigates demonstrated VNSA command and control arrangements. Due to their relative paucity, examinations of VNSA CBRN incidents are supplemented with a robust investigation into the command and control arrangements discernable in *conventional* terrorist attacks. [15] Academics have catalogued more than 87,000 incidents of terrorism, attributable to about 2,000 different groups.[16] To cover the full spectrum of VNSAs, groups are considered from all the ideological categories: Nationalist/separatist/irredentist (Ethno-Nationalist) groups; secular left-wing groups; secular right-wing groups; religious terrorist groups; and single-issue groups. [17] However, by "concentrating on actual terrorist organizations, or components of those organizations, that regularly displayed or continue to display 'operational sophistication,' project researchers have narrowed those VNSAs being considered to less than 100 groups. [18] Research is ongoing; however, it is immediately obvious that numerous factors affecting displayed VNSA command and control arrangements are largely ecumenical. These include the variables of ideology, perceptual filters, organizational structure, organizational dynamics, organizational life cycle status, relations with external actors, demographics, resources, operational capabilities, operational objectives, attack modalities, and target selection.[19]

"Nothing can be Effectively New in Touching the Course of Men's Lives That is Not Also Old"[20]

Factors influencing VNSA nuclear command and control structures are likely to be numerous. However, by identifying pertinent variables extant in social and organizational psychology, it is possible to develop theories of state nuclear command and control, and assess VNSA CBRN and conventional command and control structures, and form a framework with predictive application. Thus, subsequent aspects of the study involve "testing" the framework with subject matter experts, applying the resulting modified model to actual VNSAs, and extrapolating their likely nuclear command and control structure.

Oppenheimer observed that the scientific and military revolutions precipitated by the release of atomic energy were "surely not because…it [has] no analogue in our late history. It is precisely because that history has so well prepared us to understand what these things may mean." [21] So too, it is hoped that FAS's study will demonstrate if non-state actor nuclear command and control can be predicted—and influenced—through investigation of recent and more distant sociological, psychological, strategic, and political forces and developments. **FAS**

ENDNOTES

[1] See, for example, National Security Presidential Directive/NSPD 51, May 9, 2007. The White House, available at: http://www.fas.org/irp/offdocs/nspd/nspd-51.htm

ENDNOTES

2. For capability requirements and material procurement obstacles and opportunities see Charles D. Ferguson et al., *The Four Faces of Nuclear Terrorism* (Monterey, CA: Center for Nonproliferation Studies, 2004) and Michael Levi, *On Nuclear Terrorism* (Cambridge, MA: Harvard University Press, 2007), cf. Robin Frost, "Nuclear Terrorism After 9/11," Adelphi Papers, December 2005. For explorations of violent non-state actors' motivations for engaging in nuclear attacks see Brian Michael Jenkins, *Will Terrorists Go Nuclear?* (Amherst, NY: Prometheus Books, 2008), esp. chapters 3-5, 10, 14-15 and Jeffrey M. Bale and Gary Ackerman, "How Serious is the 'WMD Terrorism' Threat?: Terrorist Motivations and Capabilities for Using Chemical, Biological, Radiological, and Nuclear (CBRN) Weapons," report prepared by the WMD Terrorism Research Program, Center for Nonproliferation Studies, 2005, Part II on motivations.

3. The command and control elements of terrorists writ large has been explored, although much more work needs to be done in this broad area. See, for example, Brian A. Jackson, "Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and Its Application to Al Qa'ida," *Studies in Conflict and Terrorism*, Vol. 29, No. 3, April-May 2006, 241-162 and Bryan C. Price, B. "Removing the Devil You Know: An Empirical Analysis of Leadership Decapitation and Terrorist Group Duration" Paper presented at the annual meeting of the Theory vs. Policy? Connecting Scholars and Practitioners, New Orleans Hilton Riverside Hotel, The Loews New Orleans Hotel, New Orleans, LA, Feb 17, 2010.

4. VNSAs could perceive of a nuclear weapon as a political tool; a means towards statehood; an element of blackmail; a weapon of revenge, punishment, economic disruption, deterrence or last resort. Moreover, VNSAs with an apocalyptic eschatology might see nuclear weapon use as precipitating a purifying global Armageddon. For an excellent study of the nexus between such millenarian VNSAs and CBRN weapons see Robert Jay Lifton, *Destroying the World to Save It: Aum Shinrikyō, Apocalyptic Violence, and the New Global Terrorism* (New York: Metropolitan Books, 1999). See also Charles P. Blair, "Jihadists and Nuclear Weapons," in Gary Ackerman and Jeremy Tamsett, eds., *Jihadists and Weapons of Mass Destruction: A Growing Threat* (New York: Taylor and Francis, 2009), 193-195.

5. Seminal works that explore these systems include Paul Bracken, *The Command and Control of Nuclear Weapons* (New Haven, and London: Yale University Press, 1983); Bruce G. Blair *Strategic Command and Control: Redefining the Nuclear Threat* (Washington, D.C: Brookings Institute Press, 1985); Peter D. Feaver, "Command and Control in Emerging Nuclear States," *International Security*, Vol.17, No. 3 (Winter 1992/93); Bruce G. Blair, *The Logic of Accidental Nuclear War* (Washington: The Brookings Institute, 1993); and Scott D. Sagan, "The Origins of Military Doctrine and Command and Control Systems" in Peter R. Lavoy, Scott D. Sagan, and James J. Wirtz, eds., *Planning the Unthinkable* (Ithaca and London: Cornell University Press, 2000).

6. With regard to nuclear-armed state actors, Peter Feaver has described decapitation as "an enemy nuclear attack against command and control centers, particularly against the national leadership . . .which would render the [state] unable to respond even if a sizable portion of the . . . nuclear arsenal survived." Peter D. Feaver, *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States* (Ithaca: Cornell University Press, 1992), 73-74. In the case of nuclear-armed VNSAs, decapitation refers to an attack that renders the group incapable of employing (additional) nuclear weapon(s) even if in a post-attack environment the group still has possession of such weapon(s). For a seminal early discussion of decapitation see John D. Steinbruner, "Nuclear Decapitation," *Foreign Policy*, no. 45 (Winter 1981-82),16-28.

7. This is the case in both 1) preemptive attacks—those aimed at preventing an initial nuclear attack and 2) responsive assaults precipitated by a successful or attempted nuclear attack—military responses intended to prevent further nuclear attacks. The opportunities—and risks—afforded states engaging in predelegation of nuclear weapons are explored in Peter J. Roman, "Ike's Hair-Trigger: U.S. Nuclear Predelegation, 1953-60," *Security Studies* 7, no. 4 (Summer 1998), 121-164. See also, Richard H. Kohn and Joseph P. Harahan, eds., "U.S. Strategic Air Power, 1948-1962: Excerpts from an Interview with Generals Curtis E. Lemay, Leon W. Johnson, David A. Burchinal, and Jack J. Catton," *International Security*12, no 4 (Spring 1988), 78-95.

8. This study is in collaboration with the National Consortium for the Study of Terrorism and Responses to Terrorism (START), a U.S. Department of Homeland Security Center of Excellence; it is part of a multi-year START project which includes inter alia Gary A. Ackerman, Charles P. Blair, Jeffrey M. Bale, Victor Asal and R. Karl Rethemeyer, *Anatomizing Radiological and Nuclear Non-State Adversaries: Identifying the Adversary*. Report prepared for the Science and Technology Directorate, Department of Homeland Security, grant number N00140510629 (College Park, MD.: National Consortium for the Study of Terrorism and Responses to Terrorism, 2009); Gary A. Ackerman, Charles P. Blair and Maranda Sorrells, Radiological and Nuclear Non-State Adversaries Database (RANNSAD). (College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism, 2009); and Gary A. Ackerman, Charles P. Blair, and Jeffrey M. Bale, *Anatomizing Radiological and Nuclear Non-State Adversaries: Potential RN Adversary Behavioral Profiles*. Report prepared for the Science and Technology Directorate, Department of Homeland Security, grant number N00140510629 (College Park, MD.: National Consortium for the Study of Terrorism and Responses to Terrorism, 2010).

ENDNOTES

9. Robert Oppenheimer, “The New Weapon: The Turn of the Screw,” in The Federation of American Scientists’, *One World or None* (New York: McGraw Hill, 2007), 59. This volume was originally published in 1946.
10. Edgar Schein, *Organizational Culture and Leadership*, 4th Ed. (San Francisco: Wiley, 2010), passim.
11. See endnote #5.
12. Feaver, “Command and Control in Emerging Nuclear Nations,” 178.
13. Ibid, 180.
14. The “Always/Never Dilemma” captures systemic structural variables putatively encountered by states. According to Feaver all possessors of nuclear weapons, including new nuclear states, confront an inescapable dilemma. If a leader’s control of the weapons is too relaxed, deterrence can “fail deadly” in the form of an accidental or unauthorized launch. However, if control is too firm, deterrence can “fail impotent” if the leadership is decapitated and has no chance of retaliation. In differentiating between these two goals, authorities are forced to choose between a more assertive or more delegative command and control system. Feaver, “Command and Control in Emerging Nuclear States,” passim.
15. Radiological and nuclear (RN) cases, for example (including plots, attempted acquisitions, possession of materials, threats with possession, and use of RN materials as a weapon), more substantial than a mere threat number 131 incidents (as of early 2010). When excluding dubious end-users and likely apocryphal cases, the total falls to less than 80. Almost half of the perpetrators in these cases were lone actors and, with regard to all incidents, most were interdicted during their plotting phase. Ackerman, Blair and Sorrells, Radiological and Nuclear Non-State Adversaries Database (RANNSAD).
16. See START’s Global Terrorism Database (GTD), available at: http://www.start.umd.edu/gtd/.
17. See Gary Ackerman, Jeffrey M. Bale, Charles P. Blair, et al., “Assessing Terrorist Motivations for Attacking Critical Infrastructure.” Lawrence Livermore National Laboratory, UCRL-TR-227068, December 4, 2006, 16-18, available at: https://e-reports-ext.llnl.gov/pdf/341566.pdf .
18.This author is indebted to Jeffrey M. Bale and Jarret Brachman for their assistance in creating a framework that narrows incidents and groups down to those that are relevant to the study. Quotation is taken from author’s correspondence with Jeffrey M. Bale, Director, Monterey Terrorism Research and Education Program, July 29, 2010. Autonomous, “bottom-up” cells created by rank amateurs are largely immaterial to the study. This is because, “Although amateurs occasionally do manage to carry out successful and highly destructive single attacks, these are not usually marked by a high degree of sophistication, either with respect to technical or operational capabilities (e.g., the Madrid bombings). In short, the tradecraft employed by amateur, i.e., non-professional, terrorist groups is not usually of a very high order even in those relatively few cases where they are able to carry out surprisingly successful attacks.” Bale, correspondence with author.
19. For more on these key factors see, Ackerman, Bale, Blair, et al, “Assessing Terrorist Motivations for Attacking Critical Infrastructure,” 20-23.
20. Oppenheimer, “The New Weapon: The Turn of the Screw,” 59.
21. Ibid, 59-60.

Charles P. Blair joined FAS in June 2010 as Director of the Terrorism Analysis Project. An expert in radiological and nuclear weapons, Blair’s work focuses on the nexus of violent non-state actors and weapons of mass destruction (WMD). Prior to joining FAS, he was a research associate with the National Consortium for the Study of Terrorism and Responses to Terrorism where, among other projects, he managed the Global Terrorism Database, the largest open-source compilation of terrorist events in the world.

Since 2005 Blair has co-directed the Center for Terrorism and Intelligence Studies (CETIS). Largely serving the needs of U.S. governmental agencies, CETIS studies terrorist targeting and decision making as they relate to critical infrastructure vulnerability. Previously Blair served as a research associate at the Center for Nonproliferation Studies’ (CNS) Monterey Terrorism Research and Education Program and as an investigative researcher for the Anti-Defamation League (ADL).

A dual U.S./French citizen, Blair has studied in France, India and the former Soviet Union. He holds a B.A. in history from the University of Colorado at Boulder and an M.A. from the Monterey Institute of International Studies in international policy studies with a focus on the technical issues and policies surrounding WMD.

Cyber Warfare: Surviving an Attack

By Devabhaktuni Srikrishna

Cyberspace is a new domain of warfare. Created to minimize the vulnerability of United States communications networks to a crippling nuclear first strike by the Soviet Union, the Internet that was originally envisioned to enhance U.S. security is turning into a battlefield [1] for nations or sub-national groups to launch virally spreading attacks [2] and induce network failures potentially involving critical infrastructure systems.[3]

Cyber warfare and cyberoffense [4] have been a part of U.S. military operations for decades.[5] Treaties and rules of engagement define what is off-limits during a cyberwar.[6] The more vulnerable the system is, the more policy is necessary to deter adversarial nations from launching attacks, and vice-versa.

Some cyberattacks are analogous to air forces probing one another's defenses or perhaps to espionage during the Cold War, which occurred though there was no official war and no physical harm. Cyberespionage operations of China, for example, against the United States and its allies have been going on for years and will never really end.[7]

U.S. Air Force General Kevin Chilton, former Commander-in-Chief of Strategic Command, has stated that every computer system fielded by U.S. servicemen is on the front lines of a virtual battlefield.[8] Perhaps all people should think of their computer systems (PCs, mobile devices, etc) in this manner, not just as a tool for achieving personal goals but also as a conduit for an enemy attack.

This survey of cybersecurity literature explores answers to the question of how to secure the Internet from a cyberwar.

What is Cyberwar and Cyberoffense?

Richard A. Clarke and Robert Knake offer a vivid explanation of some of the largest recent cyberattacks in their book, *Cyber War: The Next Threat to National Security and What to Do About It*. Once a virus or malware is inadvertently downloaded onto a networked personal computer (PC) by a user[9], the PC can be commandeered to perform cyberattacks ranging from electronic banking crimes, politically motivated denial of service attacks[10], email spam[11], and click-fraud[12].

The U.S. Government Accountability Office (GAO) offers a taxonomy of different types of attacks in "Cybersecurity for Critical Infrastructure Protection,"[13] – denial of service, exploits, logic bombs, sniffers, Trojan horses, viruses, and worms. Attackers also employ arbitrary combinations of these attacks as part of an integrated attack plan.

Causes of Cyber Vulnerability

In "Cyberwar and Cyberdeterrence," Martin Libicki points out that system vulnerabilities do not result from immutable physical laws, but due to a gap in theory and practice. Organizations are vulnerable to the extent they want to be and to how much they want to spend to address vulnerabilities. [14] And cyber vulnerabilities can be completely eliminated -- unlike conventional, nuclear, chemical, or biological which are permanent vulnerabilities due to laws of nature.

Aside from keeping individual PCs secure and virus-free through antivirus software [15] or having Internet providers enforce anti-virus policies on their subscribers,[16] several tools with varying degrees of sophistication exist for identifying and policing unusual behavior in real-time – for individual PCs (Bothunter[17]), enterprise networks (Damballa [18]), federal government networks (Einstein [19]), and critical infrastructure (Perfect Citizen [20]). The drawback of such systems is that creative attackers continue to find ways to circumvent them. Software must be constantly updated and will at some point be outdated when the next threat emerges.

Another option is to eliminate anonymity on the Internet through end-to-end authentication in order to prevent anonymous attackers from carrying out distributed attacks with impunity.[21] While end-to-end authentication may prevent cyberattacks and identify the culprits, it would result in the loss of privacy, individual liberties, and split the Internet into multiple Internets.

As an outstanding example of loss of privacy and violation of individual liberties, cyberattacks on hospital networks are of particular concern as they deal with patient-sensitive data. In the case of medical records, system design involves backup and distributed storage – attacks that involve data destruction can be recovered if the data is routinely backed up in multiple independent locations. The lost data can be made accessible quickly and reliably after an attack. But unless stronger data protection measures are in place, the concern remains that a cyber thief can steal sensitive data that could be used to blackmail people with certain medical conditions.

Similarly there ought to be no critical infrastructure connected to the Internet left vulnerable to cyberattack. Curiously, the nuclear power industry, known for its fail-safe engineering in reactor design, is sometimes recognized as better prepared than most other industries to withstand cyber threats. It does this through upfront planning and design for isolated or disconnected operation to avoid the worst-case scenario of a reactor being commandeered by a hacker, "The safety and control systems that operate nuclear power plants are isolated from the Internet and are protected against outside invasion." [22]

Who Are the Cyberattackers?

The same Internet that allows for billions of dollars in electronic commerce can also empower a single mobile device to control millions of personal computers (PC) around the world for electronic crime. Due to its anonymous and highly scalable nature, the Internet can also be used as a weapon to disrupt and commandeer essential services that rely or connect to the Internet.

Cyberattacks can be carried out by anyone with the know-how and interest, and in many cases the cost of attacking is disproportionately small compared to the potential damage that can be inflicted. Groups involved in planning and executing attacks range from nations to individuals. Most nations would probably agree that attribution of a cyberattack is imperfect – whether it means identifying the nations involved, sub-groups, or motives. [23] Mistakes in attribution due to haste or inaccurate information can lead to collateral damage.

While the GAO summarizes potential attackers and motivations, [24] the range of possible groups and motives is much broader: criminal groups, hackers, hacktivists, insiders, intelligence agencies, terrorists, and virus writers.

Martin Libicki explained that attribution is difficult because: [25]

1. Cyberattacks can launch from anywhere, and computers do not leave physical traces behind.
2. A rogue employee or sysadmin presents risks similar to those of an attacker within the periphery of a closed system.
3. Code within the electronics supplied by third parties can bring down a system at a pre-specified time or in response to some system state.
4. When attribution is localized to a country or on government networks, it may be someone operating on behalf of what they perceive to be state interests without clear authorization from the state.
5. Organized criminals posing as governments, or "super-patriots" may be attacking in advance of what they perceive to be government actions.

An example of a cyber attack by a country or nation was revealed when the group WikiLeaks released a cache of confidential American diplomatic cables to the New York Times among several other news organizations. Some of these cables described a computer hacking effort against Google's computer system by the Chinese Politburo.[26]

This cyber intrusion was part of a global campaign to sabotage the multinational corporation and carried out by Chinese operatives and computer hackers hired by the Chinese government, according to news stories about the leaked cables.

The recent Stuxnet PC virus illustrates a cyberattack by an anonymous agent. The Stuxnet virus spread via PCs and was designed by its authors to infect and then destroy or sabotage the operation of a specific type of CPU made by Siemens and used for automated control in electric power plants worldwide including in North America, Iran, Pakistan, India, Indonesia, and Germany. [27]

Articles and weblog posts suggest that the U.S. and/or Israel[28] targeted Iran's nuclear program.[29] Attribution in the Stuxnet case is far from straightforward – unless a link or evidence is found.[30] In spite of international politics on nuclear proliferation, it is difficult to imagine the motive of a country like the U.S. to carry out such a sloppy sabotage attack – especially as the cyberattack affects reactors in many countries including the United States. [Editor's Note: As this article was going to press, the New York Times reported that Iranian President Mahmoud Ahmadinejad said that a cyberattack had damaged an unspecified number of Iranian centrifuges for enriching uranium.[31] Reportedly, Stuxnet caused the frequency of the spinning centrifuges to change so that the devices would spin out of control. Ivanka Barzashka, a research associate at FAS, was one of the first analysts to discover this feature of Stuxnet.[32]]

The attack was facilitated because systems deployed worldwide are (1) standardized on a vendor's product so the virus can replicate and (2) use of proprietary code used in the standardized platform – not benefiting from widespread peer-review (vs. open-sourced software/code).

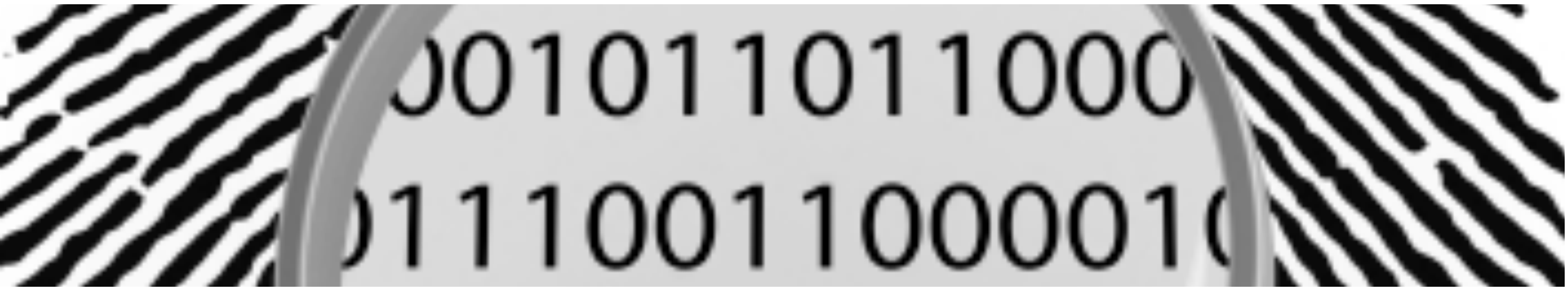
Conclusions

To secure the Internet from cyberattacks requires a combination of public policy, standardization, and market forces. Intelligent application of simple, proven engineering design principles in different situations such as end-to-end authentication, behavioral analysis, distribution (vs. centralization), backup, redundant routes (vs. single paths), fault-tolerance, diversity of supply (hardware, software, and services), and decoupling from the Internet, might eliminate the worst consequences of most vulnerabilities.

Perhaps the biggest challenge is to create secure practices for individuals and organizations that are easy to understand, adopt, and apply when designing and operating networked computer systems. [Editor's Note: FAS will continue to research this issue and provide practical policy recommendations.] **FAS**

ENDNOTES

1. Bruce Schneier, *Crypto-Gram Newsletter*, "The Risks of Cyberterrorism", June 15, 2003: http://www.schneier.com/crypto-gram-0306.html; See Schneier on Security, a blog covering security and security technology, "Cyberwar", June 4, 2007: http://www.schneier.com/blog/archives/2007/06/cyberwar.html.
2. *Christian Science Monitor*, "Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant?" by Mark Clayton, September 21, 2010: http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.
3. *Wired- Threat Level* (a blog about privacy, crime and security online), "Report: Critical Infrastructures Under Constant Cyberattack Globally" by Kim Zetter, January 28, 2010 http://www.wired.com/threatlevel/2010/01/csis-report-on-cybersecurity/.
4. *United Press International*, "Analysis: USAF's Cyber Offense Capability" by Shaun Waterman, May 15, 2008: http://www.spacewar.com/reports/Analysis_USAFs_cyber_offense_capability_999.html, and *Armed Forces Journal,* May 2008, "Carpet bombing in cyberspace: Why America needs a military botnet" by Col. Charles W. Williamson III, http://www.armedforcesjournal.com/2008/05/3375884. See also *The Economist*, "Cyberwar", July 1, 2010: http://www.economist.com/node/16481504.
5. *Foreign Affairs*, November/December 2009, "Securing the Information Highway: How to Enhance the United States' Electronic Defenses" by Wesley K. Clark and Peter L. Levin: http://www.foreignaffairs.com/articles/65499/wesley-k-clark-and-peter-l-levin/securing-the-information-highway.



ENDNOTES

6. *The Washington Pos*t, “15 nations agree to start working together to reduce cyberwarfare threat” by Ellen Nakashima, July 17, 2010: http://www.washingtonpost.com/wp-dyn/content/article/2010/07/16/AR2010071605882.html; *The New York Times,* “Step Taken to End Impasse Over Cybersecurity Talks” by John Markoff, July 16, 2010: http://www.nytimes.com/2010/07/17/world/17cyber.html; See also the news release on a special report from the Council on Foreign Relations, “U.S. Must Take Stronger Leadership Role to Protect Interests at Risk in Cyberspace, Says Council Special Report”. The *Council Special Report, Internet Governance in an Age of Cyber Insecurity,* is by CFR Fellow Rober K. Knake: http://www.cfr.org/publication/22880/us_must_take_stronger_leadership_role_to_protect_interests_at_risk_in_cyberspace_says_council_special_report.html ; *Arms Control Today*, June 2010, “Multilateral Agreements to Constrain Cyberconflict” by James A. Lewis: http://www.armscontrol.org/act/2010_06/Lewis.
7. The Parliament of Canada, Library of Parliament, Parliamentary Information and Research Service, “Cybersecurity and Intelligence: The U.S. Approach” by Holly Porteous, February 8, 2010: http://www2.parl.gc.ca/Content/LOP/ResearchPublications/prb0926-e.htm; National Journal, “China’s Cyber-Militia” by Shane Harris, May 31, 2008: http://nationaljournal.com/member/nationalsecurity/china-s-cyber-militia-20080531; *The Register [UK],* "IE zero-day used in Chinese cyber assault on 34 firms: Operation Aurora unveiled" by Dan Goodin of San Francisco, January 14, 2010: http://www.theregister.co.uk/2010/01/14/cyber_assault_followup/ ; *The Washington Post*, "Google China cyberattack part of vast espionage campaign, experts say" by Ariana Eunjung Cha and Ellen Nakashima, January 13, 2010: http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.
8. *The Register [UK]*, “Cyber attack could bring US military response” By Robert Lemos, May 13, 2009: http://www.theregister.co.uk/2009/05/13/us_cyber_attack_response/.
9. *PC World*, “Beware the Botnets” by Brian Krebs, January 24, 2010: http://www.pcworld.com/article/187532/beware_the_botnets.html.
10. *The Register [UK]*, “Botnets linked to political hacking in Russia” by John Leyden, December 14, 2007: http://www.theregister.co.uk/2007/12/14/botnet_hacktivism/.
11. *The New York Times,* “Thieves Winning Online War, Maybe Even in Your Computer” by John Markoff, December 5, 2008: http://www.nytimes.com/2008/12/06/technology/internet/06security.html.
12. UBM TechWeb’s Dark Reading website, “The Top 10 Enterprise Botnets” By Kelly Jackson Higgins, February 17, 2010: http://www.darkreading.com/insiderthreat/security/client/showArticle.jhtml?articleID=222900762 .
13. See Table 9: Types of Cyberattacks, “Cybersecurity for Critical Infrastructure Protection” http://www.gao.gov/new.items/d04321.pdf.
14. Weblog, Information Security Resources, “Debunking Cyber Deterrence as a Strategy” by Richard Stiennon, October 31, 2009: http://information-security-resources.com/2009/10/31/debunking-cyber-deterrence-as-a-strategy/.
15. StopBadware, http://stopbadware.org/.
16. On March 2, 2010, during the Microsoft Corporation’s RSA Conference in San Francisco, Scott Charney (Corporate Vice President for Trustworthy Computing) presented a keynote address titled “Why don't we think about access providers who are doing inspection and quarantine, and cleaning machines prior to access to the Internet?” http://www.microsoft.com/presspass/exec/charney/2010/03-02rsa2010.mspx.
17. Security Focus, "BotHunter aims to find bots for free" by Robert Lemos, November 25, 2008: http://www.securityfocus.com/brief/861; *The New York Times*, “Thieves Winning Online War, Maybe Even in Your Computer” by John Markoff, December 6, 2008: http://www.nytimes.com/2008/12/06/technology/internet/06security.html; *PC World,* “Monitor Botnet Threats Your Antivirus Can't See” by Robert Vamosi, February 17, 2009: http://www.pcworld.com/businesscenter/article/159706/monitor_botnet_threats_your_antivirus_cant_see.html; http://www.bothunter.net/.
18. Damballa® stops breaches by botnets and advanced persistent threats that exploit networks for illegal activity. http://www.damballa.com/.
19. See the Government Information Security website. This article was adapted from testimony presented to the House Committee on Homeland Security on the current state of the U.S. Computer Emergency Readiness Team, “Einstein Presents Big Challenge to U.S.-CERT” by Richard L. Skinner (Inspector General of the Department of Homeland Security), June 22, 2010: http://www.govinfosecurity.com/articles.php?art_id=2677; United States Government Accountability Office, Report to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, U.S. House Committee on Homeland Security, “Cyber Analysis and Warning,” July 31, 2008: http://www.gao.gov/new.items/d08588.pdf.
20. *Wall Street Journal*, “U.S. Plans Cyber Shield for Utilities, Companies” by Siobhan Gorman, July 8, 2010: http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html.

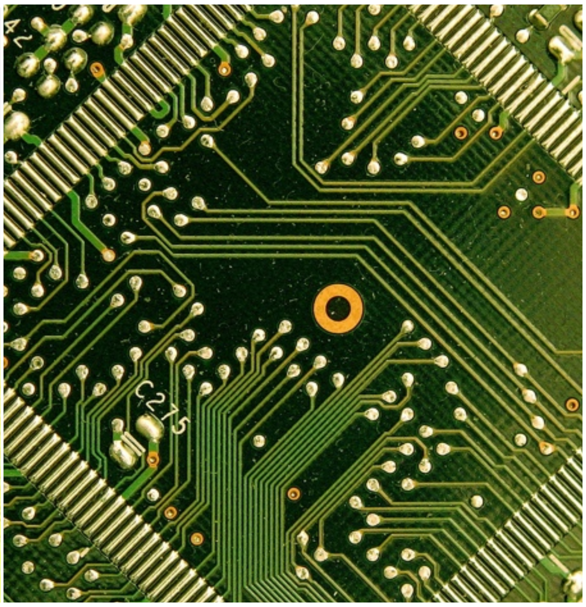
ENDNOTES

21. *The Washington Post*, "Mike McConnell on how to win the cyber-war we're losing" by Mike McConnell, February 25, 2010: http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.
22. *Global Security Newswire* [The National Journal Group], "Nation's Nuclear Power Plants Prepare for Cyber Attacks" by Martin Matishak, August 27, 2010: http://gsn.nti.org/gsn/nw_20100827_1692.php.
23. *Technology Review*, published by the Massachusetts Institute of Technology, "Russia's Cyber Security Plans" by David Talbot, April 16, 2010: http://www.technologyreview.com/blog/editors/25050/
24. U.S. General Accounting Office, Technology Assessment, see Table 6: Threats to Critical Infrastructure Threat Description, "Cybersecurity for Critical Infrastructure Protection," May 2004: http://www.gao.gov/new.items/d04321.pdf.
25. RAND Corporation, Monograph Series prepared for the U.S. Air Force, Project Air Force, "Cyberdeterrence and Cyberwar" by Martin Libicki, pages 18-21 and 71-72, 2009: http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf.
26. *The New York Times*, "Leaked Cables Offer Raw Look at U.S. Diplomacy" by Scott Shane and Andrew W. Lehren, November 28, 2010: http://www.nytimes.com/2010/11/29/world/29cables.html
27. *Christian Science Monitor*, "Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant?" by Mark Clayton, September 21, 2010: http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.
28. *Wired*, "New Clues Point to Israel as Author of Blockbuster Worm, Or Not" by Kim Zetter, October 2010: http://www.wired.com/threatlevel/2010/10/stuxnet-deconstructed/.
29. *Bloomberg/BusinessWeek*, "Computer Worm May Be Targeting Iranian Nuclear Sites" by Arik Hesseldahl, September 24, 2010: http://www.businessweek.com/news/2010-09-24/computer-worm-may-be-targeting-iranian-nuclear-sites.html; *The Economist,* "A worm in the centrifuge," September 30, 2010: http://www.economist.com/node/17147818.
30. *Global Security Newswire,* "Iran Could Limit Uranium Enrichment, Ahmadinejad Says," September 27, 2010: http://gsn.nti.org/gsn/nw_20100927_5440.php.
31. *The New York Times,* "Bombings Hit Atomic Experts in Iran Streets" by William Yong and Robert F. Worth, November 29, 2010: http://www.nytimes.com/2010/11/30/world/middleeast/30tehran.html.
32. *The Washington Post*, "Stuxnet Worm Possibly Made to Cripple Iran Centrifuges" by Glenn Kessler, 16 November 2010: http://www.washingtonpost.com/wp-dyn/content/article/2010/11/15/AR2010111506768.html.

Devabhaktuni "Sri" Srikrishna was the founder and Chief Technology Officer of Tropos Networks, which builds metro-scale wireless broadband (Wi-Fi) systems based on cellular mesh technology and is deployed in several cities across the United States. Srikrishna is a member of the FAS Board of Directors.

His publications have spanned quantum computing, parallel computing, wireless data communications, and nuclear detection.

> ***"Cyberattacks can be carried out by anyone with the know-how and interest, and in many cases the cost of attacking is disproportionately small compared to the potential damage that can be inflicted. Groups involved in planning and executing attacks range from nations to individuals."***



A Systems Approach to Yemen's Critical Environmental Issues

By Lindsey Marburger, Earth Systems Program, Federation of American Scientists

In August 2010, experts from the Earth Systems Program of the Federation of American Scientists (FAS) traveled to Yemen to inaugurate the new International Science Partnership (ISP). The pilot project in Yemen will address environmental issues critical to the United States and Yemen, build and support long-term partnerships between U.S. and Yemeni scientists and engineers, and develop Yemen's capacity to engage in meaningful environmental and security-related scientific research.

In meetings with scientists, engineers, politicians and government officials, tribal leaders, and other energy and environmental stakeholders, FAS sought answers to the following questions: What are the key environmental issues in Yemen? What are the proposed solutions? How effective, from a systems perspective, are these solutions? And how can science and technology (S&T) engagement be leveraged to solve these critical issues?

Yemen's environmental issues range from the impact of fossil fuel exploitation to urban sanitation limitations, deforestation, and marine pollution. The most pressing concern is Yemen's critical shortage of freshwater supplies, especially in the interior highland cities of Taiz and Sana'a.

Once called *Felix Arabia*, Happy Arabia, by the Romans, Yemen was long thought of as the breadbasket of Arabia, renowned for its lush green mountains and abundant agriculture. However, over the past 30 years, the traditional water management systems have broken down throughout the basin as the central government altered local management norms and as access to diesel powered pumps for wells and boreholes (largely funded through World Bank loans) dramatically increased groundwater extraction.

"In the capital city of Sana'a, located at 7000 feet with a population of 2 million and growing, eight inches of rain falls per year. Fossil reservoirs are being depleted and might empty its water reservoir in as little as a decade."

Today the Sana'a Basin, a semi-arid region covering more than 1236 square miles (3200 km^2), receives only 3-12 inches (8-30 cm) of rain per year and its primary aquifer is depleting at an unsustainable 13-20 feet (4-6 meters) annually.

For two years politicians and the news media have called attention to this problem, declaring that Sana'a will be the world's first capital city to run out of water, projecting that the aquifer will be completely depleted, leaving the city virtually waterless, by the end of the decade, or 2050 at the latest.

However, Yemen's security problems will begin well before the "all water gone" date as localized water aquifer depletion and conflict occur.

Water as a Security Threat

The Sana'a Basin has more than 2 million residents, with the majority of the population living in urban Sana'a. In Yemen as a whole and in Sana'a more than 40 percent of the population lives on less than US 2 dollars per day, one in three Yemenis suffers from malnourishment, and the population is projected to double in just over twenty years. In short, Yemen is a poor, young, and rapidly growing country beset by domestic unrest.

Water disputes have already produced casualties in 1999, 2006, and 2009 and are cited as an important factor in dozens of tribal conflicts and disagreements. As groundwater is exhausted in one area of the Sana'a Basin, this is likely to produce intense tribal conflict over access to water and water rights. The provision of water infrastructure such as wells and water

water tanks has been one of Yemeni President Ali Abdulla Saleh's key tools for consolidating his power. By doing so, he has gained legitimacy from the Sana'a governorate's tribes. Even localized groundwater depletion represents a human and an existential crisis for the Yemeni State.

Agriculture

Agriculture is responsible for 90 percent of Yemen's annual freshwater use, significantly impacting not only water use in Yemen, but water and environmental quality and pollution. To provide some perspective, agriculture in the United States consumes about 80 percent of our freshwater as a whole and 90 percent of the water in 17 western states. So while Yemen's agriculture is highly water inefficient and ultimately unsustainable, its volume of consumption is not unusual.

What is unusual is that 45 percent of the water in Yemen and over 50 percent of the water in the Sana'a Basin is used to produce qat—tree or shrub with amphetamine-like stimulating properties when chewed. This water-hungry cash crop is grown through flood irrigation, a technique that causes high levels of water evaporation and inefficiency. And while some suggest that qat may actually be less water intensive than grapes, it is without doubt more water intensive than the grain, fruit crops, and coffee it often replaces.

Proposed Solutions

The two main water shortage solutions discussed by politicians in Yemen are desalinating water from the Red Sea and pumping it to Sana'a or relocating the entire population of Sana'a to the Red Sea Coast. However, both of these solutions come with extremely high price tags—well into the billions—and neither addresses the underlying unsustainable consumption patterns. Any solution should be technical and socially transformative in nature, and must decrease consumption, drive efficiency improvements, and set up (or, where possible, revive) sustainable management mechanisms.

The Role of S&T Engagement

To address water security in a meaningful capacity, the S&T community needs to engage with Yemeni scientists and stakeholders to improve the country's capacity to undertake research in three primary areas: monitoring and modeling water resources, reducing water consumption in the agricultural sector, and developing water management mechanisms that are socially, economically, and environmentally sustainable.

The most immediate need is to improve monitoring and modeling to collect accurate data for good management plans. Research should focus on: obtaining accurate precipitation data by placing more monitoring stations throughout the basin, determining how quickly the fossil aquifer is being depleted through the plateau by integrating remote sensing water data with chemical isotope analysis of wells, and developing accurate climate models to show how precipitation will change in Sana'a over the next two decades.

In agriculture, basic and applied research is needed to find and deploy new water tolerant crops, and new technologies and techniques to improve the efficiency of the irrigation system. In addition, a study is needed to document the environmental impact of insecticides, fertilizers, and other agricultural chemicals, as well as the real water use and environmental impact and costs of qat.

With dwindling water resources and limited supply options for the Sana'a basin, management is a challenge and must be part of the water security solution. Sustainable resource use and allocation mechanisms are critical. The development of these management systems through legislation, regulations and water rights codification, markets, economic interventions, and profit sharing mechanisms will require significant scientific, legal, and social science expertise. As such, they represent one of the best opportunities for America to collaborate with Yemeni experts, politicians, and resource managers.

FAS experts continue to perform world-class analysis on the security and policy implications of resource use and availability. Simultaneously, we are working to develop solutions to key environmental security challenges by bringing together scientists in developed countries with their counterparts in developing countries.

FAS

Lindsey Marburger manages the Earth Systems Program, overseeing FAS's work in building technologies, energy efficiency and energy technology training and safety, and systems resource analysis.

Prior to joining FAS in June 2009, she worked as an energy security and economics researcher at a US-based non-governmental organization, as a grant manager at the Indo-U.S. Science and Technology Forum, and as a technical editor at Environmental Quality International. She received her Bachelor's degree from American University, where she studied environmental politics, environmental science, and applied anthropology. She has also studied at the American University in Cairo and earned her Level III Arabic certification from the Yemen Institute for Arabic Language.

BREAKING NEWS UPDATE

Before the failed Al Qaeda in the Arabian Peninsula (AQAP) plot to bomb two cargo planes bound for the United States in October 2010, foreign governments and the news media issued continuous warnings of terrorism and expressed concern whether Yemen would become the next "failed state."

In his October 29 speech, President Obama announced that the U.S. intended to "strengthen a more stable, secure and prosperous Yemen so that terrorist groups do not have the time and space they need to plan attacks from within its borders."

This statement was coupled with an announcement to increase the military aid to Yemen to $150 million, a new phase in Yemeni-U.S. relations in both rhetoric and financial commitment.

While this aid package targets many of Yemen's major destabilizing factors, it does not address key human, economic, and environmental destabilizing factors.

A more comprehensive and customized aid and engagement package is necessary. **FAS**

For more updates, please follow the Earth Systems Blog: http://www.fas.org/blog/earthsystems/

Photos by Lindsey Marburger.

To learn more about the new International Science Partnership , please visit: http://www.fas.org/programs/energy/ISP/index.html

Join FAS in thanking the Sponsors of the 2010 FAS Awards

Gold

General Atomics
HBO
Roger and Vicki Sant

Silver

Residue Regency Pad Corporation
USA Science and Engineering Festival

Bronze

Bellona USA
Lashof Family Charitable Gift Fund
Rodney W. Nichols
Arthur H. Rosenfeld
Sigma Space Corporation
Turner Foundation Inc.

Green

The Federation of Electric Power Companies of Japan
Laura Turner Seydel

FAS Launches New Program - Students for International Security (SIS)

The Students for International Security (SIS) is a new student outreach effort to provide the next generation of scientists and engineers a vehicle to further the conversation on security and science topics, and to impact policy decisions made in Washington and abroad in a nonpartisan way. The scientists who founded FAS felt they had an ethical obligation to inform and influence our country's decision makers about critical security and science issues. Today, FAS remains devoted to this idea, and believes that is our responsibility to develop this next generation so that policy makers will continue to be informed.

SIS groups provide a venue for undergraduate and graduate students, university faculty, and experts to come together to discuss important issues. Presently, three SIS groups are established: Columbia University, the George Washington University, and Murdoch University in Perth, Australia (SIS is indeed a global effort). FAS is working to expand the SIS program in the spring 2011 to universities such as George Mason University, Georgetown University, John Hopkins University, the University of Cincinnati, and many more.

Many of the FAS members are academics or technical experts in a wide variety of disciplines, teaching at major universities across the country, and holding high level positions in the non-profit, for-profit, and governmental worlds. To get involved please contact James Wright at jwright@fas.org.

To learn more about SIS, visit: http://www.fas.org/member/sis.html.

Call for Articles

In an effort to provide timely articles about security policy, nonproliferation, earth systems, educational technologies and other areas of science and technology policy, FAS members are invited to submit proposals for articles (maximum of 1,500 words).

Selection of articles is at the discretion of the editor and completed articles will be peer-reviewed.

Proposals should be sent to:

Editor, PIR
Federation of American Scientists
1725 DeSales Street, NW
6th Floor
Washington, DC 20036

Or via email to press@fas.org.

Support FAS Today

To update your membership online, please visit http://www.fas.org/member/donate_today.html.

YES I want to join the thousands of FAS members working to ensure that science and technology are used to address a broad spectrum of security issues and to promote humanitarian uses of science and technology.

Email James Wright, Manager of Development and Membership Services at the Federation of American Scientists, to learn how you can make a difference at jwright@fas.org.

Mail this form with a check to:

Membership
Federation of American Scientists
1725 DeSales Street, NW
6th Floor
Washington, DC 20036

____
EMAIL

____
First Name Last Name

____
Address 1

____
Address 2

____
City State Zip Code

____
Telephone Number Fax Number

Membership: ***Please circle the amount you would like to donate.***

$ 500 $250 $150 $100 $50 Other ________________

In the next issue of the *Public Interest Report*...

- report from the 2010 FAS Awards Ceremony honoring Dr. John Holdren and Ms. Barbara Pyle
- the launch of the new Virtual Biosecurity Center
- nuclear energy analysis by experts

The Federation of American Scientists
1725 DeSales Street, NW, 6th Floor
Washington, DC 20036