

PIR

THE MAGAZINE FOR SCIENCE & SECURITY

Summer 2012 Volume 65 No 1

Multilateral Cyber Security Solutions: Contemporary Realities

Digital Détente:
A Strategic
Response to
Cyber Espionage

SOCIAL
MOTIVATIONS
IN A CYBER
WORLD

NUCLEAR
POWER
SAFETY

DEBUGGING AMERICAN
CYBER POLICY

\$12.95US

FAS



2012 SYMPOSIUM ON PREVENTING CATASTROPHIC THREATS AND FAS AWARDS

Friday, November 9, 2012

**National Press Club
Ballroom**

529 14th Street, NW
Washington, DC 20045

TIME: 9:30 a.m. - 5:30 p.m.

RECEPTION: 6:00 - 7:30 p.m.

To register for the FAS Symposium on Preventing Catastrophic Threats and the 2012 FAS Awards, please visit:
<http://members.fas.org/2012symposium/register> .

Only three days after the national election, the Federation of American Scientists (FAS) is hosting a day-long symposium that features distinguished speakers who will present recommendations to the new administration on how to respond to catastrophic threats to national security.

Confirmed speakers include Dr. John Ahearne, Dr. Kennette Benedict, Mr. Charles Blair, Dr. Sidney Drell, FAS President Dr. Charles D. Ferguson, Dr. David Franz, Dr. Richard L. Garwin, Dr. Steve Koonin, Mr. Hans Kristensen, Dr. Robert Standish Norris, Dr. Stanford Ovshinsky, Mr. Matt Schroeder, and Dr. Paul Walker with Miles

O'Brien, science correspondent for the PBS *NewsHour*, as moderator.

FAS also is honoring outstanding scientists who have made a distinctive contribution to public policy. **Dr. John Ahearne, Dr. Sidney Drell, and Dr. Stanford Ovshinsky** will receive the 2012 Richard L. Garwin Award, the 2012 Public Service Award, and the 2012 Hans Bethe Award respectively at the awards ceremony. Dr. Drell shares the honor of the Public Service Award with **Dr. Henry Kissinger, Senator Sam Nunn, Dr. William J. Perry, and Dr. George P. Shultz.**

The award luncheon's Master of Ceremonies is **Mr. Joseph Cirincione**, President of the Ploughshares Fund.

Founded in 1945 by many of the scientists who built the first atomic bombs, FAS works at the intersection of science policy and security to promote a safer and more secure world.

To learn about **sponsorship opportunities**, please contact Katie Colten at TEL 202-454-4694 or kcolten@fas.org.

PIR

Summer 2012 Volume 65 No 1



FEATURES

10... Multilateral Cyber Security Solutions: Contemporary Realities

Cyber security poses one of the more significant contemporary challenges today, resulting in the deployment of enormous resources and countless papers and reports.

The authors examine the different forms of multilateral cooperation via various institutions. The different forms may provide better or worse contexts for achieving, or not achieving, risk reduction and agreements on what constitutes bad behavior in cyberspace.

By A. M. Rutkowski, W.A. Foster, and S. E. Goodman at the Georgia Institute of Technology.

17... Debugging America's Cyber Policy

Information leaks and faulty programming revealed to the world that the United States developed and deployed offensive cyber attacks. As details emerged, the way the U.S. weaponized cyber technology was eerily reminiscent of the way it weaponized nuclear technology 70 years ago. In both cases, the United States weaponized new technology with little understanding of the consequences for the broader international community. And yet, the United States disregarded legitimate concerns over their offensive use in favor of its perceived vital national security.

By Libby Osher, Security Scholar at the Federation of American Scientists.

23... Digital Détente: Designing a Strategic Response to Cyber Espionage

Strategic thought, from the Cold War and earlier, can be useful in addressing cyber security challenges – including cyber espionage – but only if applied with imagination and with some modification. In a curiously circular way the purpose of strategy should be to make strategy possible. The goal should be for cyber espionage to become a subject for serious, balanced public policy discourse and for cyber space itself to become a strategic arena in which diplomacy, negotiation, bargaining, compromise and concession can all have their place.

By Paul Cornish of the University of Bath.

30... Social Motivations in a Cyber World

In terms of cyber security policy, officials are writing legislation for outdated technology. By the time the legislation that is being written now is enacted, the technology will have advanced significantly according to Moore's Law.

By Clair Strom, Federation of American Scientists, and Monica Amarello, Managing Editor, Federation of American Scientists.

RESEARCH REPORT

32... Nuclear Power Safety: Lessons From Three Mile Island and the Fukushima Reactor Accidents

Of accidents that have involved nuclear-power reactors, all have ultimately delivered useful lessons about nuclear safety, reactor design, and radiation effects. This article describes some overlooked autonomous nuclear instrumentation that can be installed to independently measure reactor water levels and fissile fuel distribution — before, during, and after an accident.

By Alexander DeVolpi



Summer 2012 Volume 65 No 1

ESTABLISHED 1945

CHARLES D. FERGUSON
Editor in Chief

MONICA A. AMARELO
Managing and Creative Editor

EDITORIAL BOARD

Gilman Louie, Rosina Bierbaum, Philip B. Carter,
David Franz, Alton Frye, Robert G. Gard, Jr, Richard L.
Garwin, Nathaniel Goldhaber, Lisa Gordon-Hagerty, Lawrence M. Krauss, Rodney W. Nichols, Scott Sagan, Maxine
L. Savitz, Michael L. Telson, Valerie Thomas

LETTERS TO THE EDITOR

FAS Public Interest Report

1725 DeSales Street, NW

6th Floor

Washington, DC 20036

PHONE: (202) 546-3300

FAX: (202) 675-1010

EMAIL: pir@fas.org

The PIR welcomes letters to the editor. Letters should not exceed 300 words and may be edited for length and clarity.

Annual subscription is \$50.00 per year. Archived FAS Public Interest Reports are available online at www.fas.org.

FOR ADVERTISING Call (202) 454-4680.

Copyright 2012 by the Federation of American Scientists.

CONTRIBUTORS

MONICA AMARELO

She is the director of communications for the Federation of American Scientists

PAUL CORNISH

Professor Cornish is professor of international security at the University of Bath. He is a member of the UK Chief of the Defense Staff's Strategic Advisory Panel, and has contributed to a number of Parliamentary inquiries.

ALEXANDER DEVOLPI

Dr. DeVolpi is a retired nuclear physicist with almost 40 years of experience in reactor instrumentation, experimental diagnostics, and specialized technology at the Argonne National Laboratory, near Chicago, Illinois.

WILLIAM ABBOTT FOSTER

William Abbott Foster is a senior research associate at Georgia Tech's CISTP. Between 1995 and 2001, he was International Policy Editor or CIX, the world's first Internet Service Provider Association.

SEYMOUR E. GOODMAN

Seymour Goodman is professor of international affairs and computing at the Sam Nunn School of International Affairs and the College of Computing, Georgia Institute of Technology. He also serves as Co-Director of both CISTP and the Georgia Tech Information Security Center (GTISC).

LIBBY OSHER

She is a master's degree candidate in nonproliferation and terrorism studies at the Monterey Institute of International Studies and a Security Scholar at the Federation of American Scientists where she researched cyber security and bioterrorism.

MARK RAIZEN

Professor Raizen has held the Sid W. Richardson Chair in physics at the University of Texas at Austin since 2000. He is a Fellow of the American Physical Society and the Optical Society of America. Prof. Raizen pioneered the study of quantum chaos with cold atoms.

ANTHONY M. RUTKOWSKI

Tony Rutkowski is a distinguished senior research fellow at the Georgia Institute of Technology's Center for International Strategy, Technology, and Policy (CISTP) at the Sam Nunn School of International Affairs.

FRANCIS SLAKEY

Dr. Slakey is the associate director of public affairs for the American Physical Society. He is also The Upjohn Lecturer on Physics and Public Policy and the Co-Director of the Program on Science in the Public Interest at Georgetown University.

CLAIR STROM

She is a biomedical engineering student with a pre-law minor at Stevens Institute of Technology in Hoboken, NJ. During the summer of 2012, she studied law and public policy at Georgetown University and interned at the Federation of American Scientists.

FAS.ORG

FAS ONLINE

Secrecy News

Read reports on new developments in government secrecy and access resources on secrecy, intelligence and national security policy.

www.FAS.org/blog/secrcy



Podcasts

FAS staff and experts from outside the institution contribute to FAS podcasts. These podcasts do not represent an FAS institutional position on policy issues. The "Conversation With an Expert" covers a wide variety of issues and timely science policy topics.

www.fas.org/podcasts/

ScienceWonk Blog

ScienceWonk

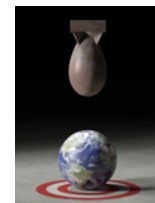
Outside experts and leaders write for this FAS blog. To be contribute to this weblog, please email a brief bio and past clips to press@fas.org.

www.FAS.org/blogs/sciencewonk

SSP Blog

Expert opinions and analyses of important national and international security issues.

www.FAS.org/blog/ssp



2012 NATO Security Summit



On May 20 - 21, 2012, the 2012 NATO Security Summit was held in Chicago. Heads of state from 28 countries convened to discuss regional and global security challenges.

NATO will not order a reduction of its nuclear arsenal but reaffirm a deployment of nearly 200 U.S. non-strategic nuclear bombs in Europe that were left behind by arms reductions two decades ago.

Visions Apart?

Although no one expected NATO to simply disarm, the reaffirmation of the current nuclear posture nonetheless falls far short of the visionary and bold initiatives that U.S. and Russian presidents took 20 year ago when they ordered sweeping reductions – and eliminations – of entire classes of non-strategic nuclear

weapons deployed in Europe and around the world.

How will NATO create the conditions for further reductions and a world without nuclear weapons? The seven-page Deterrence and Defense Posture Review (DDPR) report released in Chicago will ask the North Atlantic Council (NAC) to task its committees to “develop concepts for how to ensure the broadest possible participation of Allies concerned in their nuclear sharing arrangements, including *in case NATO were to decide to reduce its reliance on non-strategic nuclear weapons based in Europe.*” (Emphasis added).

To learn more please visit:
<http://www.fas.org/blog/ssp/2012/05/nucleargroundhog.php>

Making the Case for Nuclear Power in the United States



Will nuclear power in the United States flourish or fade away? To paraphrase Mark Twain, “The news of nuclear power’s demise has been greatly exaggerated.” The United States still has the largest number of nuclear reactors in the world with 104 and almost 20 percent of its electricity is generated from nuclear power. Moreover, four new reactors are under construction: two at the Vogtle plant in Georgia and two at the Summer plant in South Carolina. One big reason these plants are moving forward is because the utilities can recoup some of the costs during construction. The regional regulatory authorities in the Southeastern United States have allowed such cost recovery. Four new reactors, however, will not be enough to keep nuclear power on pace to continue to generate about 20 percent of the nation’s electricity.

Utilities that don’t have the cost recovery option are less likely to build new nuclear plants because of the increasing competition from cheap and abundant natural gas, especially the bonanza of gas unlocked by hydraulic fracturing in recent years. Also, the U.S. nuclear fleet has entered its middle age with a retirement cliff looming in 20 years.

Reactors initially received a license for 40 years of operation. The average age of U.S. reactors is well past 30 years. While almost all plants that have applied for a 20-year license extension have been granted such from the Nuclear Regulatory Commission, it will be a much bigger stretch to extend reactors’ ‘lives even further despite nuclear technologists’ interest in doing so. After 60 years of operations, reactor pressure vessels would have experienced intense damage from neutron bombardment. Investment in continuing R&D could ultimately result in discovering techniques to cost-effectively repair this damage and extend the life of the plants. While needed, this will not result in new plants.

For more plants to be built, nuclear power will have to make the case based on the three legs of the energy policy triangle: economics, security of supply, and the environment.

Concerning the economic assessment, the problem nuclear power faces is short-term high capital costs versus the long-term favorable financial payoff for well-run plants. In particular, the capital costs for construction can account for 60 to 70 percent of the total lifecycle costs while operations, maintenance, fuel, and decommissioning make up the remaining relatively small fraction. Because investors have perceived nuclear power construction as risky, they have demanded a high-risk premium be paid on their investments. This drives up the financing costs. The federal government has offered a few tens of billions of dollars of loan guarantees to ease the financing. But relatively high credit fees to obtain the loan guarantees have made several utilities reluctant to apply. A longer term financing mechanism could help such that investors would reduce the interest rate they demand in the short term but would reap more profit in the long term over the 60-year life of a reactor. Such a mechanism, though, runs counter

The United States also needs more wind and solar power, which are renewable sources. But the choice is not either these or nuclear power. Americans need both. The intermittent wind and solar sources can complement base-load sources such as nuclear power. A base-load source can run at constant high-level power for a relatively long period before shutdown for maintenance. Natural gas also complements these other sources because a gas power plant can run at either peaking or base-load operations. Peaking power sources can be turned on quickly to meet rapid changes in electricity demand.

Regarding security of supply, nuclear power provides a “good news” story. While the uranium needed to fuel the current fleet of reactors comes largely from foreign sources, these supplier states are mostly very friendly to the United States. Also, uranium is very dense and thus easy to stockpile. Moreover, utilities can greatly reduce the risk of supply disruptions by staggering fuel contracts among the handful of major fuel suppliers. If one supplier reneges on a contract, another supplier can meet the demand.

Next year, the nuclear fuel deal with Russia will expire. This Megatons-to-Megawatts deal will have converted 500 metric tons of uranium from Russian nuclear weapons to nuclear fuel for about half of the U.S. reactors. The expiration of this deal could stimulate revival of the U.S. domestic uranium mining and milling industry or could spur growth in uranium imports from Australia, Canada, and Kazakhstan, the three biggest global suppliers, or from other suppliers. The bottom line is that there is no need for concern about a shortage of uranium supplies for decades to come.

Although commercial nuclear power does not have a perfect environmental record due to major contamination from the 1986 Chernobyl accident and the 2011 Fukushima Dai-ichi accident, I would argue that, on balance, nuclear power is a comparatively wise choice from an environmental perspective. No nuclear plant is inherently safe, but the most modern plants are safer than the older generation plants. And safety improvements on the older generation plants can significantly reduce the likelihood of accidents and mitigate the environmental consequences if an accident occurs. Concerning emissions from plants during normal operations, a nuclear plant emits no greenhouse gases. In comparison to coal plants, nuclear power plants do not emit toxic arsenic or mercury. Coal plants produce mountains of coal ash while nuclear plants result in highly radioactive waste that is much more compact in its volume. This radioactive waste will decay to relatively low radioactivity levels in a few hundred years whereas coal ash will last forever. According to the September 2010 report “The Toll from Coal,” by the Clean Air Task Force, coal plants in the United States will contribute to more than 13,000 premature deaths. Barring major accidents and massive releases of radioactive contamination, nuclear power is comparatively benign.

If the external environmental and health costs from coal plants were included in its price, nuclear power would become cost competitive. Even without that explicit extra cost to coal, a case can and should be made for more nuclear power plants in the United States.

Charles D. Ferguson
President, Federation of American Scientists

NATIONAL SECURITY NEEDS
BRAINS.
THE FEDERATION OF AMERICAN SCIENTISTS
FAS KNOWS THAT.
ITS EXPERTS ARE
WORKING TO
ENSURE THAT WE ARE BEING
SMART
ABOUT OUR SAFETY AND SECURITY
AND HAVE BEEN SINCE 1945.



JOIN US



<http://www.fas.org/member/index.html>

STAY INFORMED



www.FAS.org



www.Facebook.com/FAScientists



Twitter.com/FAScientists



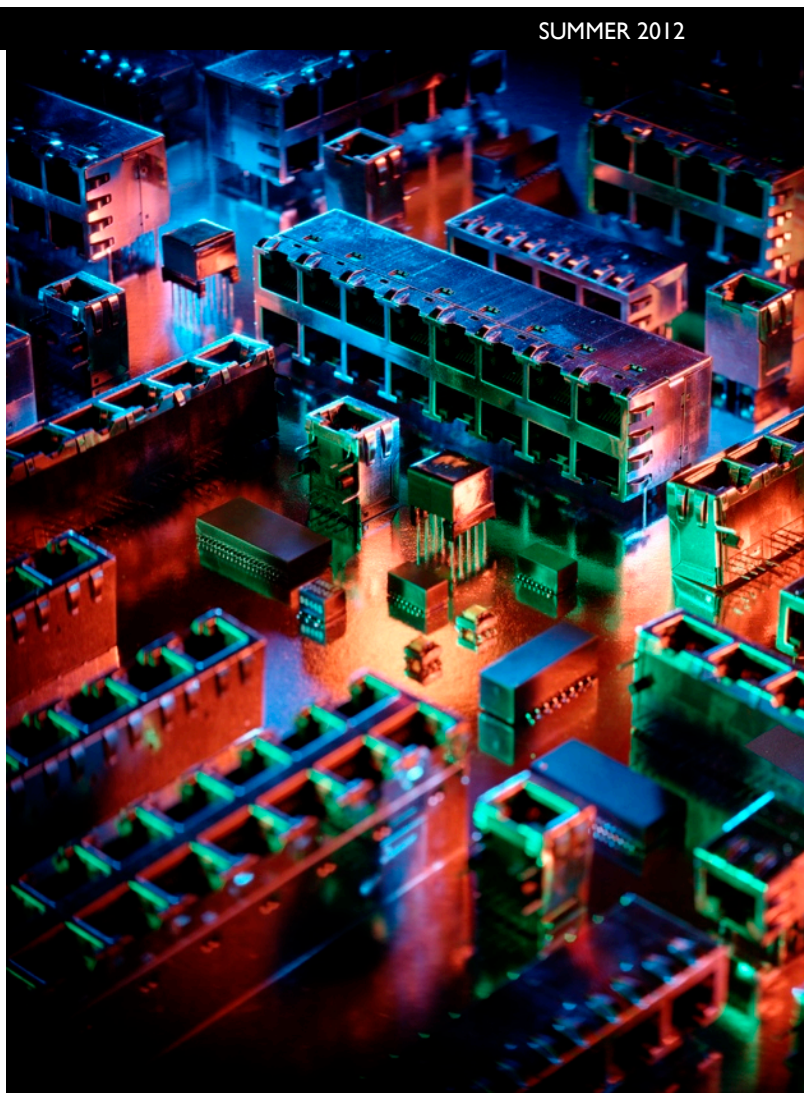
www.FAS.org/blogs.html



www.FAS.org/podcasts.html

Multilateral Cyber Security Solutions: Contemporary Realities

— BY A.M. RUTKOWSKI,¹
W.A. FOSTER,² S.E. GOODMAN³



Cyber security poses one of the more significant contemporary challenges today, resulting in the deployment of enormous resources and its treatment in countless papers and reports. Inevitably, the subject of multilateral solutions is treated—suggesting the need and efficacy of pursuing or evolving various forms of global agreements and activities. One of the more comprehensive recent analysis is the now two-year old Sofaer-Clark-Diffie paper from the U.S. National Research Council Committee on Deterring Cyberattacks, Workshop on Informing Strategies and Developing Options.⁴

Using that paper and other related material as a starting point, we examine the nature and evolution of international collaborative activity related to cyber security since its publication — with a focus on multilateral solutions. Our brief report here is intended as an examination of the different forms of multilateral cooperation via the

various institutions in the context of the extremely complex domain of cyber security. The different forms may provide better or worse contexts for achieving, or not achieving, various forms of risk reduction and agreements on what constitutes bad behavior in cyberspace.

There are two points emerging from this examination. The first is that in the realm of cyber security, a formal multilateral group with a huge mixed membership like the International Telecommunication Union (ITU) is not the place for operational security activities. Communities of trust in cyber security are both endemic and essential—many highly compartmentalized. This essential need is not found in more generic multilateral venues. The second point is that emerging functional cyber security platforms are “triple use.” The same platforms that are essential for network management and for cyber security, are also used for surveillance by all governments. These three uses inher-

ently engender very different trust communities that are context dependent and evolve through time—sometimes abruptly. It should also be pointed out that these platforms can be used by all manner of nimble criminal or antisocial actors.

This article also describes what appear to be new important attributes and constraints on that activity which inevitably limit and shape future multilateral solutions. This includes cyber security platforms that have emerged such as Continuous Security Monitoring as well as the increasing use of extraterritorial action to deal with non-state actors.

Cyber Security Fundamentals

At the outset of any review of cyber security—given the myriad different abstractions in use—it is essential to describe a definitive construct for purposes of its treatment here.

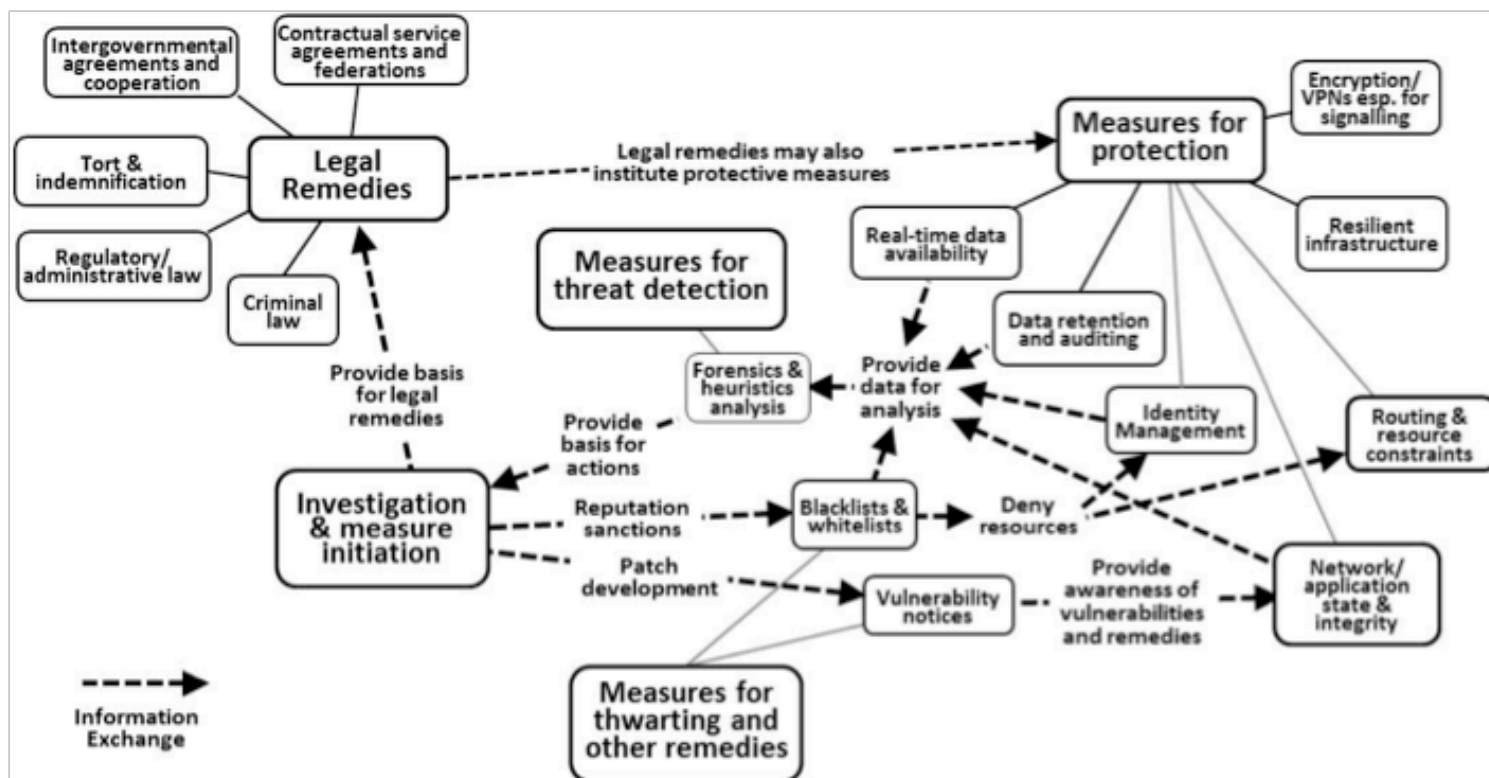


Figure 1. A model for describing cyber security.

The definition provided here is a simplified derivative of the many complex ones that have been formally adopted.⁵

Cyber Security consists of sets of techniques, policies, and activities intended to enhance trust and mitigate vulnerabilities inherent in the complex networked devices and services that permeate our lives today.

The Lukasik-Goodman-Rutkowski graphic depiction, developed four years ago, is also helpful in portraying what techniques and activities are comprised by cyber security. The diagram depicts cyber security as five clusters of interrelated activities: measures for protection, measures for threat detection, measures for thwarting and other remedies, investigation and measure initiation, and legal remedies. Highly dynamic and time critical information exchanges occur among the components of this highly distributed, autonomous cyber security ecosystem.

The model is essential because of an emergent reality. All of the devices that constitute or are attached to our informa-

tion communication networks today consist of ever increasing numbers of subcomponents and executable lines of code to provide some exponentially growing numbers of services, applications and other functional capabilities counted in the millions. There are billions of such devices. All of these entities are continuously and autonomously changing—facilitated by openness in most networked devices and services that further exacerbate the complexities and vulnerabilities. The sheer number of potential threats and exploits in this environment preclude them ever being known. They also remain constantly evolving, ubiquitous, and persistent.

Added to this mix of system vulnerabilities and threats are institutional and human elements. Actors ranging from nation states to isolated individuals are capable of creating or exploiting vulnerabilities in these environments. Indeed, a knowledgeable insider in even an otherwise closed network environment is frequently one of the most difficult threats to detect and remedy. The result is a constantly changing exercise in risk assessment and reduction.

Absolute or even a strong measureable form of security is not possible. Important members of the cyber security community announced in December 2011 that that “there’s no such thing

as ‘secure’ any more...”⁶ Subsequently much of the cyber security community has settled on Continuous Monitoring (CM) as the best we can do on a large scale at this time.⁷ CM itself consists of numerous platforms such as Security Content Automation Protocol (SCAP) and an array of related assurance and incident exchange standards and practices designed to accomplish three things:

- (1) constantly assessing the risk state of all devices and systems,
- (2) constantly watching for threats,
- (3) effecting remediations as soon as possible.

It assumes that there is no absolute security, and that the best we can do is manage risk. The Continuous Monitoring platform is the principal ensemble mechanism for advancing all of these capabilities. Underpinning the CM ensemble are structured information exchanges at known trust levels. CM is now diffusing through numerous industry and government collaborative forums worldwide.

Collateral Effects of the Continuous Monitoring Paradigm

Continuous Monitoring has arguably emerged as the principal viable approach for dealing with cyber security on a global scale. This new paradigm also has the collateral effect of reshaping and constraining multilateral solutions. The benchmark test for all multilateral solutions is: do they reduce cyber security threat risks. Unfortunately many multilateral organizations are ill equipped to do this operationally. While such organizations may have the capability for getting agreement on broad goals in legislative settings or even common specifications, they are not only ineffective at operational roles among compartmentalized trust communities, but also may adversely affect the risk equation by possibly adding more threats from the interposed multilateral organization itself.

For example, intergovernmental organizations in particular are highly vulnerable to insider treats. Organizations are beholden to fixed requirements for established nation states that treat all countries and their staff as equal and at the same trust level. Because staff are sponsored and approved by their nation states, the result is that broad global multilateral organizations in the UN system have rather low trust levels that presume the existence of extensive insider threats. North Korean staff is assumed to have the same trust level as staff from the United Kingdom.

The concerns here are not new. The Sofaer-Clark-Diffie analysis treated a number of requirements to improve multilateral organizations. One factor was “trust.” They noted that cyber security is highly dependent on dynamic trust communities. The analysis noted that the U.S. had a decided preference for dealing among allies, “rather

than through a multilateral arrangement with states that have different agendas and are less trusted.”⁸

Continuous Monitoring substantially exacerbates the trust concerns. Highly time sensitive and trusted actionable information is constantly needed, and that is something which multilateral organizations are notoriously bad at. In organizations like the ITU, even relatively benign national telecommunication statistical information has been provided well after deadlines and regarded as so manipulated that it created secondary opportunities by third party companies and agencies to compile more trustworthy statistics.⁹ Indeed, multilateral organizations are generally bound to accept provided information as fact and cannot

independently question what they receive. Even where the multilateral organization might be providing the information based on some third parties, the organization may be introducing a further element of distrust by imposing itself in the middle.

The Flame Incident as a Multilateral Trust Challenge Example

On May 31, 2012, ITU Secretary-General Hamadoun Touré issued a press release announcing via a special relationship with the Russian cyber security firm Kaspersky Labs that the ITU was assisting the Iranian government with newly discovered malware dubbed “Flame,” and that his office intended to play a leadership role to deal with new global cyber security threats.

Flame is a prime example of why governments and industry must work together to tackle cyber security at the global level. Early warning of new threats is vital and it is critical

that best practice on required corrective steps is shared in order to best protect the global information society. This is the value in building a global coalition.¹⁰

What Touré apparently didn’t know or wasn’t told is that Flame was relatively common surveillance software that multiple cyber security organizations had been following and not a new massive global security challenge nor a threat to the “global information society.”¹¹ Indeed, the day before the ICSCERT (Industrial Control Systems Computer Emergency Response Team) and the USCERT (United States Computer Emergency Readiness Team) released a joint advisory detailing its characteristics, explaining that it was designed to steal information, was confined, and described how to mitigate its propagation.¹²

The next day the *New York Times* published a front-page article based on anonymous high-level U.S. government sources, described a broad program of software based agents designed to support global actions for limiting nuclear weapons proliferation.¹³ Although the details are not entirely known, it appears as if Flame may have been deployed by some governments to assess and watch for nuclear security threats. Subsequent press coverage and online discussion has continued to question the ITU actions in the matter and its role.¹⁴

Additional Impediments to Multilateral Solutions

CM is not the only factor that has an important effect on the use of multilateral solutions.

National borders are largely irrelevant and non-state actors abound in the cyber security realm. In fact, the non-state actor challenge worldwide has led to nations such as the U.S. adapting centuries old maritime and warfare law to create new doctrines of “long arm jurisdiction.” Such adaptations of old law have been applied to an array of “kinetic” initiatives, such as the use of drone aircraft, and is arguably a necessary means for dealing with non-state actors in the cyber security realm.

It is not realistic for large multilateral organizations to provide comparable capabilities because of need to coordinate resources among multiple nations in real time.

Cyber security technology is also dual use. Some of the same techniques that are used for cyber security can be used for surveillance of adversaries—both domestic and foreign—and are indeed marketed as such by vendors. The knowledge and expertise largely exists in the private sector and in a few state security communities. Large multilateral organizations have no effective means of compartmentalizing their information. As a result, no rational state is likely to dispose of its strategic advantages in these areas by making actionable information available to every other nation in the world through a multilateral organization.

Operational Network Security Roles Are Historically Difficult

As Sofaer-Clark-Diffie noted, there is no real multilateral body today in the field of information networks. Even in eras when the technology was less complex, multilateral organizations such as the ITU were unable to deal with relatively simple “cyber security” conflicts. Going back to the initial 1850 Dresden Convention on the Electrical Telegraph, a general escape clause was inserted that the signatories may avoid any specified treaty obligation when national security interests were at stake.

Over the years, when disputes did arise—for example, in the radio spectrum domain which is functionally an open global network similar to the Internet—the ability of the ITU to resolve disputes was usually not possible. Many states such as the U.S. refused categorically to accept any ITU dispute resolution jurisdiction.¹⁵

One particularly outstanding institutional example of a failed dispute resolution mechanism consisted of the International Frequency Registration Board, created in the spirit of multilateral idealism in the late 1940s. The Board barely got started before the Cold War began and the interest in its ability to perform a quasi-judicial role to resolve disputes over spectrum usage all but disappeared. For the past 50 years it has remained as essentially a dormant organ of the ITU.¹⁶



Useful Multilateral Organization Roles

There are significant roles to be exercised that have demonstrated value over many years and across multiple institutions. The most prominent and enduring of these value propositions are agreements on the technical formats and capabilities for exchanging cyber security information within diverse trust relationships. This approach is exemplified in ITU sector work, the Convention on Cybercrime, and a number of other multilateral cyber security activities today.

An example of multilateral cyber security activity that has provided global value, while avoiding counterproductive operational roles, has been ongoing in the ITU’s technical standards body—the ITU-T—for the past three years. It has been successful in pulling together cyber security experts and bodies to assemble the specifications for techniques and activities intended to enhance trust and mitigate vulnerabilities. The activity involved almost constant, extensive “social networking” style collaboration with other groups where the real cyber security work has been ongoing among large numbers of companies and experts who participate in their own specialized forums.

These specifications dubbed CYBEX (Cyber Security Information Exchange) were published and continue to be advanced in the IETF (Internet Engineering Task Force), FIRST (Forum of Incident Response and

Security Teams), and other bodies in collaboration with ITU-T which provides for broader outreach and consensus. They are based on actual specifications in use, and specifically include the most advanced current techniques for exchanging detailed technical information concerning Flame-like malware and other threats as well as their remediation. Continuous Monitoring is included. This work focused—as the name implies—on getting global agreement on “structured expressions” for exchanging in a coherent fashion, all manner of cyber security information and avoids duplicating specifications existing elsewhere.

Cyber security operations tend to be especially complex and sensitive as the actual exchange of the information inherently involves diverse compartmentalized trust communities who constantly collaborate among themselves.

The Cybercrime Convention is comprised of member states worldwide and has 47 signatories of which 35 have ratified. It establishes predicates for signatories in terms of their internal capabilities as well as contacts. The Council of Europe provides secretariat repository and other services. The Convention did not create an operational organization, but only the predicates for information exchange and trust relationships among its signatories.¹⁷ Its signatories also meet annually and share views on global developments that will affect them, and the secretariat does significant outreach and



research to assist potential signatories. The Convention has an expert and active secretariat. It helps get countries to agree to definitions of criminal cyber behavior and incorporate that and procedural law into their national laws.¹⁸

Additional examples of effective multilateral cooperation ensuing over the past several years include the establishment of the Common Criteria Recognition Agreement (CCRA) and its creation of the Common Criteria Development Board (CCDB) among more than 20 nations.¹⁹ The Common Criteria is the driving force for the widest available mutual recognition of secure IT products. Recently, the CCDB has begun moving forward to promulgate and implement the Continuous Monitoring and SCAP suites.²⁰

The NATO Consultation, Command and Control (C3) Agency has also been successful as a multilateral organization in moving forward with implementations among a broad ensemble of allies under the aegis of a Cyber Defense Data Exchange and Collaboration Infrastructure (CDXI).²¹ The emphasis in NATO is generally oriented around assessing risk and managing trustworthiness. CDXI's special value is its ability to demonstrate how to successfully implement CM and share in-

formation within a strong multilateral security alliance among a diverse membership.

The European and Information Security Agency (ENISA) provides a mechanism for achieving cyber security solutions under the EU Treaty of Rome among member states. It has come to play an important role over the past two years in identifying institutions and exchanging related information similar to other multilateral endeavors.²² Its focus includes European CERTs, CIIP and resilience, identity and trust, risk management, secure applications and services, and stakeholder relations. One of its important roles is to serve as a common means for coordinating the national CERTS within Europe.

The Forum of Incident Response and Security Teams (FIRST) is a private international organization that consists of many national governmental organizations dealing with incident response and remediation.²³ Strictly speaking, FIRST is not a multilateral organization but one that deserves status of "quasi-governmental" because of the extent to which governments are involved, as well as its uniqueness and extensive role in the cyber security arena. FIRST has also been given International Organization status by the ITU nation state members.

Notably, FIRST includes the National Computer Network Emergency Response Technical Team / Coordination Center of China (CNCERT/CC). The CNCERT plays the principal role within China in dealing with cyber security responses—particularly with external bodies—and hosts related expert workshops.

In addition to coordinating and facilitating responses to cyber threats and attacks among its different trust groups, FIRST maintains its own Special Interest Group standards forms for developing CM related standards. The Computer Vulnerability Scoring System (CVSS), for example, operates in conjunction with the Computer Vulnerabilities and Exposures (CVE) standard to enable the only global means for exchanging vulnerability information and assessing the associated risks. FIRST was created in 1989 and now consists of 260 teams across 55 countries.

What all of these multilateral activities in cyber security have in common is their focus on the technical formats and capabilities for exchanging information within diverse trust relationships. ■

Tony Rutkowski is a Distinguished Senior Research Fellow at the Georgia Institute of Technology's Center for International Strategy, Technology, and Policy (CISTP) at the Sam Nunn School of International Affairs.

William Abbott Foster is a Senior Research Associate at Georgia Tech's CISTP. Between 1995 and 2001, he was International Policy Editor or CIX, the world's first Internet Service Provider Association.

Seymour Goodman is Professor of International Affairs and Computing at the Sam Nunn School of International Affairs and the College of Computing, Georgia Institute of Technology. He also serves as Co-Director of both CISTP and the Georgia Tech Information Security Center (GTISC).

REFERENCES AND NOTES

¹ Tony Rutkowski is a Distinguished Senior Research Fellow at the Georgia Institute of Technology's Center for International Strategy, Technology, and Policy (CISTP) at the Sam Nunn School of International Affairs. As EVP for Yaana Technologies, he has served as rapporteur for cyber security at the ITU-T since 2009 and served as the counselor for two ITU Secretary-Generals between 1988 and 1992, co-authored a published ITU history, and led development and authored many cyber security standards and instruments as an engineer-lawyer over many years in multiple settings. See www.ngi.org. He can be reached at trutkowski@netmagic.com.

² William Abbott Foster is a Senior Research Associate at Georgia Tech's CISTP. Between 1995 and 2001, he was International Policy Editor or CIX, the world's first Internet Service Provider Association. He can be reached at Willam.Foster@inta.gatech.edu.

³ Seymour Goodman is Professor of International Affairs and Computing at the Sam Nunn School of International Affairs and the College of Computing, Georgia Institute of Technology. He also serves as Co-Director of both CISTP and the Georgia Tech Information Security Center (GTISC). Immediately before moving to Georgia Tech in 2000 he was director of the Consortium for Research in Information Security and Policy (CRISP) at the Center for International Security and Cooperation, Stanford University. He can be reached at Seymour.Goodman@cc.gatech.edu.

⁴ Abraham D. Sofaer, David Clark, and Whitfield Diffie, *Cyber Security and International Agreements* in Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, at 179-206, http://www.nap.edu/openbook.php?record_id=12997&page=179.

⁵ See, e.g., ITU-T Rec. X.1205, Overview of Cyber Security (04/2008), <https://www.itu.int/rec/T-REC-X.1205-200804-I>

⁶ See <http://www.net-security.org/secworld.php?id=10333>

⁷ See NIST, Continuous Monitoring Workshop., http://scap.nist.gov/events/2011/cm_workshop/presentations/index.html. See especially, Continuous Monitoring Definition and Enterprise Architecture, Steve York, NSA. See also, NIST Continuous Monitoring FAQ, <http://csrc.nist.gov/groups/SMA/fisma/documents/faq-continuous-monitoring.pdf>; NIST Publishes Draft Implementation Guidance for Continuously Monitoring an Organization's IT System Security, <https://www.itu.int/rec/T-REC-X.1205-200804-I>.

⁸ Ibid at 193.

⁹ See, e.g., Telegraphy, <http://www.telegeography.com>; CIA Factbook, <https://www.itu.int/rec/T-REC-X.1205-200804-I>

¹⁰ See http://www.itu.int/net/pressoffice/press_releases/2012/34.aspx

¹¹ See [http://en.wikipedia.org/wiki/Flame_\(malware\)](http://en.wikipedia.org/wiki/Flame_(malware)). See also, <http://www.hackingteam.it/>

¹² See http://www.us-cert.gov/control_systems/pdf/JSAR-12-151-01.pdf

¹³ See <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?ref=stuxnet>

¹⁴ See http://www.nytimes.com/2012/06/04/technology/cyberweapon-warning-from-kaspersky-a-computer-security-expert.html?_r=1

¹⁵ The instrument is known as the Optional Protocol on the Compulsory Settlement of Disputes Relating to the Constitution of the International Telecommunication Union, to the Convention of the International Telecommunication Union and to the Administrative Regulations Geneva, 1992. The accessions are reported in the Annual Report of the Activities of the ITU, Table IA.

¹⁶ See the candid historical treatment on the ITU-R website at <http://www.itu.int/ITU-R/information/promotion/e-flash/4/article7.html>

¹⁷ See Convention on Cybercrime and related materials at the COE secretariat, <http://conventions.coe.int/Treaty/en/Treaties/html/185.htm>, <http://www.coe.int/what-we-do/rule-of-law/cybercrime>



REFERENCES AND NOTES

¹⁸ See <http://www.coe.int/what-we-do/rule-of-law/cybercrime>

¹⁹ See Common Criteria Portal, <http://www.commoncriteriaportal.org/>

²⁰ See S. Barnum, Secure Content Automation Protocol (SCAP), MITRE, <http://www.yourcreativesolutions.nl/ICCC12/p/110928/C02-Sean%20Barnum.pfd>

²¹ See Luc Dandurand, *Cyber Defence Data Exchange and Collaboration Infrastructure (CDXI)*, http://www.itu.int/dms_pub/itu-t/oth/06/35/T063500000200516PPTE.ppt; *Presentation to the ITU-T Cybex Working Group*, Cambridge, MA, 13 July 2011.

²² See ENISA - Securing Europe's Information Society, <http://www.enisa.europa.eu/>

²³ See <http://www.first.org>

JOIN FAS TODAY!

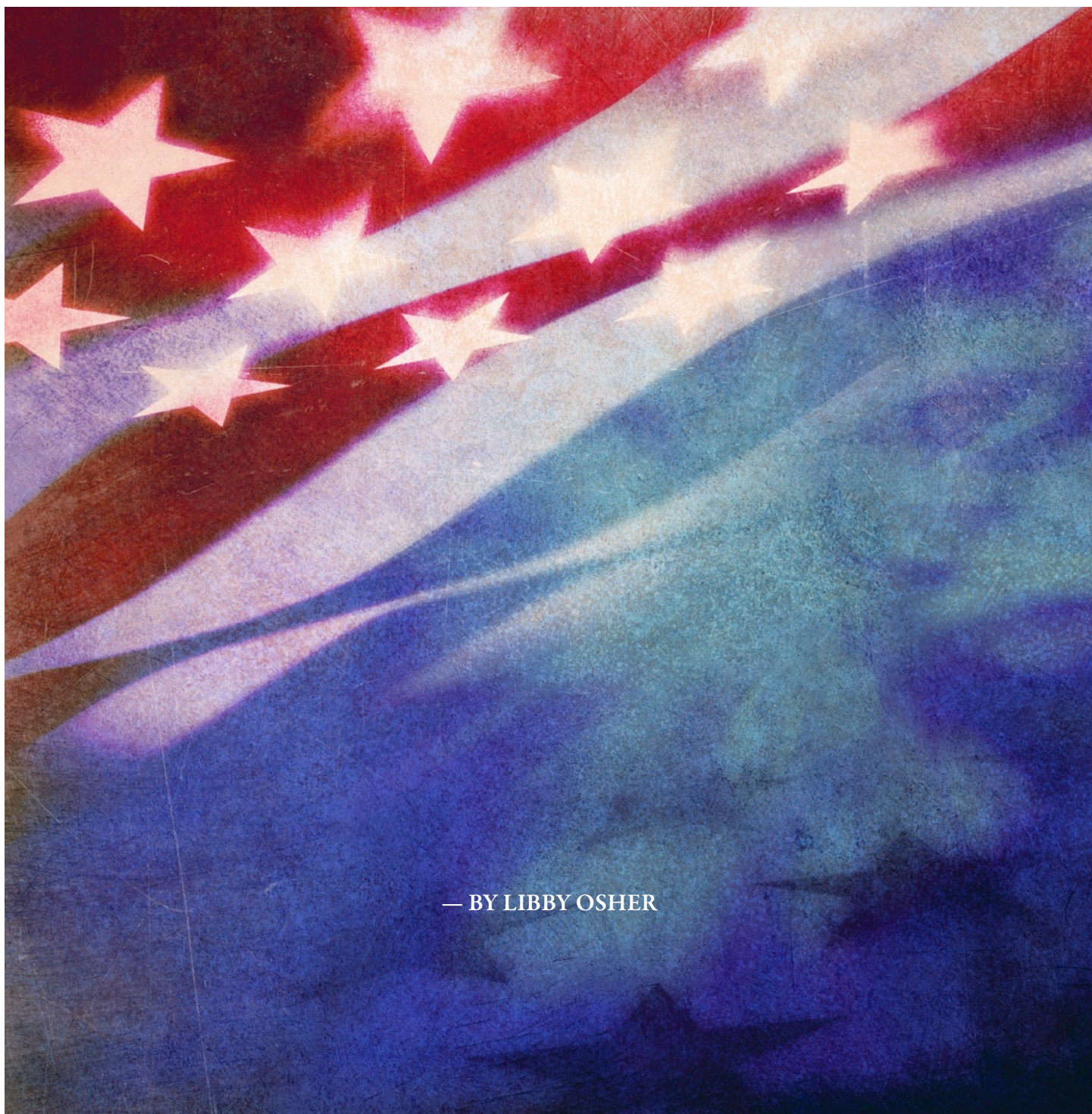
With a donation of \$50 or more, you can be an **FAS Member**, which includes a subscription to the *PIR*.

For more information on how to join the Federation of American Scientists, please contact Katie Colten at kcolten@fas.org or visit: www.FAS.org/member/index.html.

Your FAS Membership includes:

- early access to four issues of the *PIR*, the magazine for science and security;
- invitations to FAS events and briefings;
- advance notice of all FAS reports; publications and podcasts;
- direct access to science policy experts through conference calls and live chats;
- weekly information updates via email; and
- the knowledge that you are supporting an organization that is building on its prestigious legacy by performing rigorous analysis of today's most important security and science policy issues.

Debugging America's Cyber Policy



— BY LIBBY OSHER

Information leaks and faulty programming¹ revealed to the world that the United States developed and deployed offensive cyber attacks. Although it wasn't discovered until late 2010, Stuxnet was deployed at least in 2009 and was probably developed as early as the end of the Bush administration.² As details emerged, the way the U.S. weaponized cyber technology was eerily reminiscent of the way it weaponized nuclear technology some 70 years ago. In both cases, the United States weaponized new technology with little understanding of the consequences for the broader international community. And yet, the United States disregarded legitimate concerns over their offensive use in favor of its perceived vital national security:³ war with Japan and Iranian nuclear proliferation.⁴

Stuxnet is a highly sophisticated U.S.-Israeli computer worm that corrupted centrifuges at Iran's nuclear facility in Natanz. It is a complex piece of malware designed to inject code into SCADA (industrial control systems), all the while hiding its presence from the operator. Stuxnet's ultimate goal was to reprogram these industrial control systems and sabotage the centrifuges.

When the U.S. dropped the bomb on Hiroshima in 1945, it signaled to the world that nuclear weaponization was possible and acceptable. States soon scrambled to assemble their own offensive nuclear programs.

It is a complex piece of malware designed to inject code into SCADA (industrial control systems), all the while hiding its presence from the operator. American cyber attacks send a similar message that the offensive use of cyber technology could become a norm. Russia and China are sure to ramp up their cyber programs in response to American aggression⁵ leading

all three to cite the other's programs as justification for their own, just as American and Soviet nuclear regimes did less than a decade ago. Without immediate action, another arms race-driven by short-term paranoia, will occur at the expense of long-term national security.

In the years that followed World War II, there was a window of opportunity when international controls were still theoretically possible, but neither the U.S. nor the USSR made sufficient efforts to establish them. A nuclear arms race ensued, and today no less than nine countries possess nuclear weapons.⁶

It is impossible to know if a greater effort to instill international control through efforts like the Baruch Plan would have succeeded in avoiding, or at least containing, the Cold War conflict. The establishment of norms is a far

domain hasten the need for a comprehensive strategy and international cooperation. The United States must act to safeguard its virtual networks.

While there are some parallels, the weaponization of nuclear and cyber technology is very different in regards to their peaceful and military functions. Unlike nuclear material, for example, the Internet is a universal and fundamental service relied on by many institutions and integral to the daily lives of billions of people worldwide, not to mention hundreds of millions in the United States. In addition, the Internet is vital to the world economy, including essential industries such as electricity providers and financial institutions.

The average American will never handle radioactive material like uranium (U-235) or plutonium (Pu-239), let alone a nuclear weapon, but most will use the Internet. Public education of safe computer practices must be emphasized and marketed as a first line of defense against cyber attacks.

Despite habitual use, most people — from teenagers to Fortune 500 corporations — do not practice safe online behavior and sometimes fall victim to the most basic Internet scams.⁷ For example, phishing emails bait the recipient to provide confidential information and often include malicious links to websites infected with malware. While victims could avoid this scam by displaying the true hyperlink or researching the purported sender, these attacks are prevalent and costly.

The pervasiveness of phishing attacks demonstrates the vulnerability of cyber technology. In 2007, a multitude of cyber attacks were attributed to non-state actors like criminal organizations, terrorists, and hackers, including the April 2007 denial of service attack on Estonia and major intrusions of the Departments of Defense, Homeland Security, State, and Commerce.⁸ These groups and individuals benefitted from the accessibility of cyber technology, the low operational cost, and the abundant technical expertise available to launch a sophisticated cyber attack, in comparison with the deployment of a nuclear weapon.

The value of anonymity also allows states to benefit from the potency of cyber warfare. While terrorists tend to take credit for their attacks, states benefit from this

The average American will never handle radioactive material like uranium (U-235) or plutonium (Pu-239), let alone a nuclear weapon, but most will use the Internet.

easier task than to outlaw existing capabilities.

Fortunately, this is the preliminary stage of cyber warfare and there is still time to formulate domestic policies and establish international regulations. The more accessible, under-regulated, and poorly understood features of the cyber



aspect, which is completely unattainable in the nuclear arena. While nuclear technology is confined to state-level policy, the increased opportunity for abuse by diverse actors in cyber necessitates the adaptation of a defensive policy. Conventional retaliatory measures effective in the deterrence of a nuclear attack would not work against targets that cannot be identified, or punished with the tools used to address state aggression. This dynamic threat requires a revised national security policy.

Non-state actors invade cyber space instead of a nuclear weapons depot because states have monopolized nuclear technology since its inception, safeguarding it from abuse through efforts such as the Nunn-Lugar program and Global Threat Reduction Initiative. Apart from a few regulatory committees, such as the Internet Engineering Task Force (IETF) which sets technical standards for internet protocol and the Internet Corporation for Assigned Names and Numbers (ICANN) which assigns domain names, cyber space has remained largely inde-

pendent of government control.⁹ Because of their limited role in the regulation of cyber technology, governments must make every effort to avoid backroom deliberations and open up policy decisions to think tanks, private technology firms, and industries that specialize in cyber security. Discussion of cyber regulations and policy should include input from the public. Policymakers need to ensure that regulations do not trample on civil liberties or violate a right to privacy on the Internet.

While the destructive power of a cyber attack pales in comparison to the physical devastation of a nuclear weapon attack, the insidious nature of virtual attacks can have numerous lasting effects, which include the economic toll of intellectual property theft, infiltration of military databases, and the disruption of financial systems. The possibility of infiltrating a cyber network to facilitate a remote physical attack on the command and control centers of a power grid or worse, a nuclear site, is very much alive.

Corporations lose time and money spent on innovation when designs are stolen and counterfeited, which includes the violation of intellectual property rights and can ultimately

result in the loss of jobs. According to the FBI, intellectual property theft costs American businesses billions of dollars every year.¹⁰ In 2010 Yu Qin and Shanshan Du stole GM hybrid vehicle trade secrets in order to sell the information to Chery Automobile, a Chinese automotive manufacturer and foreign competitor of GM. GM estimated that the value of the stolen documents was more than \$40 million.¹¹ And in 2009, Chinese hackers infiltrated military databases to access the design of the Joint Strike Fighter (F-35) by Lockheed Martin.¹²

Cyber security norms and best practices need to be established before non-state actors carry out a lethal attack and before states develop large-scale offensive cyber programs. On the global stage, the U.S. should collaborate with the international community to call for the categorical prohibition of cyber attacks directed at power grids. An effective treaty will include monitoring and enforcement measures. Any legally binding contract will require immediate implementation, before an attack is carried out.

The potential for disaster is very real. The greater accessibility of cyber weapons to non-state actors, advantage of anonymity for states, and absence of stigma against an attack increases its likelihood and compounds the importance of the cyber policy debate. National dialogue, international cooperation, and regulations on cyber activity that mirror the policy response to nuclear weapons must be emphasized. However, the need to learn from nuclear security strategy should not be misconstrued as advocacy of the same policy constructs used to address previous forms of warfare. The Cold War doctrine should

not be applied to cyber warfare, just as pre-industrial age war-gaming strategies would not be applied to post-industrial military operations. ■

Libby Osher is a master's degree candidate in nonproliferation and terrorism studies at the Monterey Institute of International Studies and a Security Scholar at the Federation of American Scientists where she researched cyber security and bioterrorism. In 2011, she

graduated from the George Washington University with a BA in international affairs with a regional concentration in the Middle East, and a minor in Semitic languages. In her third year at GWU, Libby spent a semester at the American University of Cairo in Egypt where she focused on Arab and Muslim political and religious movements and furthered her Arabic language studies.



REFERENCES AND NOTES

- ¹ Rosenbaum, R. (2012, April). "Richard A. Clarke on Who Was Behind the Stuxnet Attack," *Smithsonian Magazine*, April 2012: <http://www.smithsonianmag.com/history-archaeology/richard-clarke-on-who-was-behind-the-stuxnet-attack.html>
- ² Falliere, N., Liam O. Murchu, & Eric Chien. (February 2011). W32. stuxnet dossier. Symantec: Version 1.4
- ³ Glenny, Misha. "A Weapon We Can't Control," *The New York Times*, June 24, 2012: <http://www.nytimes.com/2012/06/25/opinion/stuxnet-will-come-back-to-haunt-us.html>
- ⁴ Benedict, Kennette. "Stuxnet and the Bomb," *The Bulletin of the Atomic Scientists*, June 15, 2012: <http://thebulletin.org/web-edition/columnists/kennette-benedict/stuxnet-and-the-bomb>
- ⁵ Steinbruner, John D. (2011). *The Cybersecurity Situation*. CISSM working paper, Center for International and Security Studies at Maryland, University of Maryland, College Park.
- ⁶ Kristensen, Hans. Status of World Nuclear Forces, FAS.org, 2012: <http://www.fas.org/programs/ssp/nukes/nuclearweapons/ukestatus.html>
- ⁷ Boulton, Clint. "CIOs: DNSChanger Malware Won't Knock Us Offline," *Wall Street Journal*, July 8, 2012: <http://blogs.wsj.com/cio/2012/07/08/cios-say-dnschanger-malware-will-not-knock-us-offline/>
- ⁸ Lewis, J. A., Langevin, J. R., McCaul, M. T., Charney, S., & Raduege, H. CSIS Commission on Cybersecurity for the 44th Presidency, (2008). Securing Cyberspace for the 44th Presidency. Washington, DC: Center for Strategic and International Studies.
- ⁹ Nye Jr, Joseph S. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Winter 2011, p. 30: <http://www.au.af.mil/au/ssq/2011/winter/nye.pdf>
- ¹⁰ Federal Bureau of Investigation, Intellectual Property Theft: <http://www.fbi.gov/about-us/investigate/cyber/ipr/ipr>
- ¹¹ Federal Bureau of Investigation, Detroit Division, Press Release, "Two Charged in Conspiracy to Steal GM Trade Secrets," July 22, 2010: <http://www.fbi.gov/detroit/press-releases/2010/dc072210.htm>
- ¹² Gorman, Siobhan. "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, April 21, 2009: <http://online.wsj.com/article/SB124027491029837401.html>



Letters to the Editor

**FAS wants to hear
from you.**

The PIR welcomes **Letters to the Editor**. Letters should not exceed 300 words and may be edited for length and clarity.

FAS Public Interest Report
1725 DeSales Street, NW
6th Floor
Washington, DC 20036
PHONE: (202) 546-3300
FAX: (202) 675-1010
EMAIL: pir@fas.org

Listen and Learn Podcasts

FAS records
“Conversations with Experts”
on a wide range of topics.

Download
the
interviews:
[www.FAS.org
/podcasts/
index.html](http://www.FAS.org/podcasts/index.html)



Internships for a More Secure World

FAS staff are experts and recognized as leaders in their respective fields. Let FAS teach you how to work in science policy and get things accomplished.

For more information visit:
www.FAS.org/about/intern.html

make
your
mark





Digital Détente:

Designing a Strategic Response to Cyber Espionage

— BY PAUL CORNISH

Cyber Espionage

Cyber espionage – “the use of information technology systems and networks to gather information about an organization or a society that is considered secret or confidential without the permission of the holder of the information”¹ – has been rising steadily to the top of the security policy agenda. Specialist cyber security organisations report a yearly escalation in

cyber attacks; the 2011 edition of Symantec’s *Internet Security Threat Report*, for example, records a 93% increase in the volume of web-based attacks between 2009 and 2010.² Also industrial and commercial organizations, which might in the past have been reticent about admitting failure and vulnerability, are now more willing to divulge security breaches. In the words of the director of security research at Trend Micro, “more attacks are being publicly disclosed. Victims are more willing to come

forward and say something bad happened to us”.³

If the victims of cyber espionage and crime are becoming more willing to divulge their vulnerability, there is also an increasing propensity to “name and shame” the source of these attacks. The turning point is widely supposed to have occurred in 2010 when Google revealed that Chinese hackers, in a campaign known as “Operation Aurora,” had penetrated it. But that move had been anticipated some months earlier

by Richard Clarke, a former special adviser on cyber security to U.S. President George W. Bush, and someone known for his bleak assessment of the cyber security challenge. “Information technology experts in and out of government” wrote Clarke in May 2009, “believe that American corporations are regularly losing to foreign cyber espionage (most likely China’s) what gives U.S. firms their competitive edge: the results of expense on R&D, engineering plans, chemical and biological formulas, complex software, even customer lists and pricing data.”⁴

Private sector concerns about Chinese cyber espionage reached a crescendo in spring and summer 2011. The British industrialist James Dyson warned that “Chinese students are infiltrating British universities to steal technological and scientific secrets and even planting software bugs to relay the information to China. I’ve seen frightening examples. Bugs are even left in computers so that the information continues to be transmitted after the researchers have returned home.”⁵ The Chinese embassy in London refuted Dyson’s claim as “shocking and entirely unfounded and illogical” and a “damaging slander to all Chinese students.”⁶ But McAfee, another cyber security organization, then accused a single “state actor” of a long-running series of cyber attacks against an unusually wide variety of more than seventy organisations including the United Nations, the Association of Southeast Asian Nations and various defence contractors. Although McAfee did not name China as the culprit, “independent security experts” were reported to believe that “Beijing was the most likely culprit.”⁷

As well as a distinct sharpening of attitudes within the private sector, there is also mounting evidence that the public policy establishment is becoming less reticent about identifying the sources of cyber espionage. In June 2009 an article in the *New York Times* reported the concern of unnamed “United States officials” in the

recently formed Obama administration that “a significant proportion of the attacks against American government targets are coming from China and Russia.”⁸ Similarly, in the UK the Secretary of State for Defence warned in June 2011 that the Ministry of Defence faced “cyber-war attacks on a daily basis” and that “our national intellectual property in defence and security industries is at risk from systematic marauding” originating in China.⁹ The UK Security Service was reported, also in June 2011, to have accused China of devoting “considerable time and energy trying to steal our sensitive technology on civilian and military projects and trying to obtain political and economic intelligence at our expense.”¹⁰ And in October 2011 the head of cyber

For all the discussion of cyber espionage it remains, in policy terms, curiously primitive — as if its development has been arrested in a pre-strategic condition.

security in the UK Ministry of Defence warned that “The biggest threat to this country by cyber is not military, it is economic.” Claiming that “the Chinese pose the biggest threat” the official went on to observe: “If the moment you come up with a brilliant new idea, it gets nicked by the Chinese then you can end up with your company going bust.”¹¹ Both the style and the substance of this comment were reprised some weeks later when Mike Rogers, the Republican chairman of the U.S. House of Representatives Permanent Select Committee on Intelligence, claimed that Chinese hackers and spies “are stealing everything

that isn’t bolted down, and it’s getting exponentially worse.”¹² Just months earlier, the U.S. Office of the Director of National Intelligence (DNI) had published a report which asserted, with undiplomatic frankness that “the computer networks of a broad array of U.S. government agencies, private companies, universities, and other institutions – all holding large volumes of sensitive economic information – were targeted by cyber espionage; much of this activity appears to have originated in China.”¹³

The rhetoric has been escalating steadily to the point that an international confrontation is becoming conceivable, with all the disruption and harm that might entail. Given the value placed on digital communications this is scarcely a comfortable prospect. It is legitimate therefore to ask what should be done, if not to resolve that confrontation then at least to manage it as it becomes more entrenched.

For some, the Cold War can provide useful lessons in crisis management among adversaries and there is a growing interest in extending Cold War strategic thought – particularly deterrence – into cyber space. But it is at this point that things become complicated. For all the discussion of cyber espionage it remains in policy terms curiously primitive, as if its development has been arrested in a pre-strategic condition: it is not easily located on the security policy/strategic spectrum; it is notoriously difficult to attribute; and the tools with which it might be managed are not readily identifiable.

If Cold War strategic thought is to contribute to the cyber espionage debate it will require some modification. The aim should be to move cyber espionage from non-communicative adolescence into something like a mature strategic relationship, which can then be stabilised and improved. The “attribution problem,” discussed below, is the greatest impediment to this shift. In cyber space generally, and particularly in the field of cyber espionage, the most prized assets are anonymity, deniability and uncertainty and it is hard to imagine a strategic relationship developing under such conditions. An imaginative application of deterrence thinking can, however, move the cyber espionage debate in the right direction, creating a strategic relationship, which can then be managed, in the digital equivalent of détente.

The Attribution Problem

In its various guises, the cyber security debate is bedevilled by the problem of attribution; the difficulty (some would say impossibility) of establishing with sufficient confidence the identity and location of an attacker. This in turn makes it difficult to penetrate the “plausible deniability” defence behind which any cyber aggressor (cyber-spy, cyber-terrorist, cyber-criminal and perhaps even a “cyber-warrior”) can hide. Discussion of Chinese cyber espionage provides a good illustration of the problem.

In broad terms there are three contending perspectives on the question of Chinese cyber espionage. The first, which could hardly be more alarming, was offered at a conference organized by the Jamestown Foundation in Washington in February 2011. Here, the Chinese were described as “seeing digital attacks differently than U.S. planners.” China would play a “long game” in which they would, essentially, prepare the battlefield for a subsequent, more tradi-

tional conflict by ensuring that U.S. supply and logistic chains could be degraded at the critical moment. In order to infiltrate core networks, China would allow exported hardware to be inspected for security but would then “introduce malicious software via upgrades, maintenance, and other post-buy actions.”¹⁴ Others have similar suspicions. A report published in late 2010 by the *Economist* newspaper wondered whether “cyber weapons” could serve as “an ‘assassin’s mace’ in a surprise attack designed to smash America’s elaborate but fragile electronic networks. That would leave American forces half-blind and mute, and its bases and [aircraft] carriers more vulnerable still.”¹⁵

The second perspective is altogether more skeptical. The answer to the question “Why should China be involved in cyber espionage?” might begin with two observations: first, as is widely acknowledged, the barriers to entering the world of cyber espionage are relatively low; and second, as is also generally accepted, China has very high levels of high quality human capital in in-

formation and communications technology. If China has indeed become one of the world’s most active practitioners of cyber espionage, rather than ask why this is taking place the better question might be “Why should China *not* be undertaking widespread cyber espionage?” Cyber espionage could be considered an entirely rational activity, insofar as it confers so-called “asymmetric” advantages for a growing economy and offers a level of insurance against an uncertain and undecided future. By this view, Chinese cyber espionage might be much less than the early warning of an impending global confrontation. China might, instead, be doing what any other state would do in similar circumstances – exploiting what it perceives to be a passing strength until its adversaries, competitors and partners improve their performance and the “playing field” of international cyber security and commerce is levelled. As Joseph Nye has observed, “in the area of industrial espionage, China has had few incentives to restrict its behaviour because the benefits far exceed the costs.”¹⁶



The third perspective is that Chinese cyber espionage is little more than an alarmist concoction of the West's own making, designed to privilege certain departments or agencies of government over others or to make the case for government spending on this or that equipment or capability; a digital-age reprise, perhaps, of the "military-industrial complex" of the early Cold War. By one view, fears of Chinese cyber expertise are wildly exaggerated, with China more accurately ranked "near the bottom of the table" of comparative national cyber power.¹⁷ And as Amitai Etzioni has observed, there is always the risk that the persistent description of China as a sophisticated cyber-adversary will at some point become a self-fulfilling prophecy.¹⁸

For as long as accurate attribution is considered to be both critical to the policy debate yet at the same time largely unattainable, it is difficult to decide which of these three perspectives is the most reasonable. The attribution problem makes it hard to judge with enough confidence whether or not China is involved in cyber espionage and, if so, what its motives might be. It is for this reason that I describe

the cyber espionage debate as being in a state of arrested development; held at the level of speculation rather than strategy. The consequences of this are more than merely analytical, however. While cyber espionage remains under-developed and opaque as a strategic problem, it also remains impervious to careful management. And so it becomes ever more difficult to develop a cooperative relationship with cyber adversaries and competitors, rather than a relationship which might be either unnecessarily confrontational or unwisely complacent.

Deterrence and Détente

The Cold War showed how mutual deterrence could stabilize a confrontational strategic relationship.¹⁹ Without that stability it would not have been possible for détente, the more progressive idea, to gain any pur-

chase. Cold War deterrence came in two models. The first, "deterrence by punishment," functioned by threatening such a devastating response to any nuclear attack that the potential attacker would be persuaded not to proceed. Punitive deterrence of cyber espionage is less straightforward, however. Asymmetric deterrence – i.e. nuclear deterrence of a non-nuclear attack, or military deterrence of a non-military incursion – was always a complicated proposition. And given the attribution problem it is even more difficult to imagine that a large-scale military response would be made in the face of an opaque cyber attack of some

There is always the risk that the persistent description of China as a sophisticated cyber-adversary will at some point become a self-fulfilling prophecy.

sort. Nevertheless, the idea is never entirely discounted; the United States, for example, is reported to have come to the conclusion that "computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the United States to respond using traditional military force."²⁰

The second model, "deterrence by denial", sought to influence an adversary's decision calculus in a less direct manner by showing that defensive preparations would make the costs of mounting a successful attack so high as to outweigh any benefits. Here, the relevance to cyber espionage is more obvious; governments and the private sector already take defensive and preventive measures to protect their cyber capabilities. Sometimes described as "active cyber defence,"²¹ these measures could range from improved and more open working between

the public and private sector to make the information infrastructure more resilient (given that most of the infrastructure upon which government and national security, and indeed the national economy depend is privately owned),²² to the continued development of Computer Emergency Response Teams at the national and multilateral level.²³ Measures such as these, together with improved network and data security and other physical and personnel security measures, could all affect a potential cyber-adversary's assessment of risk and reward. In other words, these measures would make clear that the target state or organization is not only aware that it is the victim of espionage but is also taking measures to make it less likely that espionage will succeed, or that a far greater investment will be required if it is to do so.

Cold War deterrence – by the threat of punishment and by denial – stabilized the strategic confrontation and made it fit for détente. Détente was an attempt by Cold War protagonists to reintroduce trust in a confrontational strategic relationship which, during the 1960s and 1970s, was becoming ever more strained and prone to miscalculation, with the prospect of devastating results. Détente did not survive much beyond 1980, but at its core was a simple yet compelling idea which has not disappeared from strategic memory. To an important extent, what motivated détente was a view of the world as a commons, severe damage to which would be felt generally. By the 1960s, the nuclear arsenals of the United States and the Soviet Union were increasingly being designed to ensure that neither side would lose in a nuclear exchange. The claim of détente, conversely, was that widespread and severe devastation resulting from a nuclear war would mean that neither side could be said to have won.

It is at this point that the analogy between cyber espionage and the Cold War becomes rather stretched. During the Cold War it could not reasonably be denied that the East-West confrontation existed ideologically, politically and militarily, and there was an urgency to managing and resolving that confrontation. But these things cannot of course be said of a non-attributable cyber confrontation. In one respect, however, the Cold War analogy remains useful; the notion of a vulnerable commons, the protection of which will be to mutual benefit.

The claim that cyber space can be understood as a “global technological commons”²⁴ can elicit an allergic response in some analysts who point out that unlike oxygen, rain, the wind and the high seas, cyber space is not a naturally occurring phenomenon. Cyber space is instead a system of machines which are built, owned and maintained by people – Andrew Blum writes compellingly of the “physical infrastructure” of the Internet.²⁵ Yet what is striking about cyber space – and relevant for this article – is that its users behave as though it were indeed a benefit in common; for most users, the technology has become indispensable while the cost has been driven down to the marginal. As a result, in commercial jargon the “users” and “customers” of cyber space have come to see themselves as “stakeholders” and even “guardians” of a facility to which they have a right.²⁶ “Earthrise,” the first image of the earth taken from space in December 1968 stimulated the growth of the environmental movement and added to the pressure for strategic détente. The digital-age equivalent of that moment is the perception that the global communications and commercial infrastructure is owned in

common and must be protected. It is this idea which should motivate strategic thought in the digital era. Whereas Cold War détente was concerned in part to prevent the destruction of the highly valued physical commons, digital détente should be concerned to prevent the breakdown of the global technological commons. Two versions of deterrence can bring cyber espionage closer to this point: “deterrence by interdependence” and “deterrence by association.” Both constitute a norm-building exercise for cyber space around which a stable strategic relationship can be built. Once built, that relationship can be amenable to a digital equivalent of détente.

Deterrence by interdependence begins from the commonplace argument that national interests are best secured through the shared pursuit of an open, fair and regulated cyber space. Most national economies are irreversibly inter-connected in the global economic system and it is therefore in the interest of those states that there should be a functioning global economy with international trading partners, as well as a reliable international information and communications infrastructure.

It follows that states should be wary of cyber espionage and similar activities which might be costly and which might damage the global digital economy and themselves in the process. A state which undertook cyber espionage would not only have to be technologically proficient so as to escape detection, it would also have to be sufficiently robust so as to manage the economic shocks and turbulence that would result. There is also the question of economic resilience to consider. Although the theft of intellectual property might appear to compensate for certain disadvantages in the short term, as Adam Segal has observed it must be difficult to build and maintain a genuinely innovative and dynamic economy “when you’re busy stealing intellectual property.”²⁷

If deterrence by interdependence prefers certain behaviours and prohibits others, deterrence by association takes the norm-building exercise to the next level by emphasising the diplomatic, political and reputational damage that can result from being seen to tolerate, support or gain from pariah behaviours. This is neither a novel nor a complex idea, and is already at work in the field of nuclear proliferation: “if states and commercial organisations can be exposed for having supplied a nuclear weapon capability to a terrorist group, they can then be subject to sanctions; and the threat of sanctions might have the effect of cutting off supply in the first place.”²⁸ For deterrence by association to work, a number of steps must be taken. Public and private sector organisations which have been the victim of cyber espionage must be more forthcoming about the incidence of cyber espionage attacks and, particularly, about the level of harm caused. The victims should also be willing to discuss, in public, their best estimates of the origin of a cyber espionage attack, who or what might have orchestrated it and who might have gained from it. The purpose of the exercise would be to re-engineer the cyber espionage debate in a subtle way, by developing the norm that association with such behaviours would be reputationally damaging and should therefore be avoided. As the norm becomes more established so the onus would be placed on governments to demonstrate that they were not involved, as sponsors or beneficiaries, in cyber espionage or in any given event, rather than to argue that their involvement cannot be proved. The attribution problem will remain, certainly. But the core argument of deterrence by association (not “deterrence by *proof*”) is that a political, rather than a



technological standard of evidence can and should be used and that governments and the private sector should be encouraged not just to form judgements but to discuss them more openly as encroachments on the commons.

Conclusion

In his analysis of cyber relations with China, Amitai Etzioni assesses the relative merits of the “adversarians” against the “engagers.” “The first group” observes Etzioni, “tends to consider the rise of China as threatening to the United States interests and the world order.” The “engagers” on the other hand, tend “to consider China as a nation that seeks to focus on its own development and can be engaged to work with the United States and other nations to advance shared interests and the common good.”²⁹ Etzioni’s operating assumption, clearly, is that there is a strategic relationship with China which is susceptible to management in one direction or the other. The contention of this article, however, is that strategic relationships must first be made before they can be stabilised and improved. Yet at present, and as a consequence of the attribution problem,

relationships between cyber adversaries and competitors are at best pre-strategic; held in a state of arrested development.

Strategic thought, from the Cold War and earlier, can be useful in addressing cyber security challenges – including cyber espionage – but only if applied with imagination and with some modification. In a curiously circular way, at this early stage in the development of cyber security as a strategic problem, the purpose of strategy should be to make strategy possible. The goal should be for cyber espionage to become a subject for serious, balanced public policy discourse and for cyber space itself to become a strategic arena in which diplomacy, negotiation, bargaining, compromise and concession can all have their place. In its various forms, deterrence can assist in this process. Deterrence can be both protective and defensive, as well as constructive of a more sophisticated and progressive relationship with an adversary or competitor. Deterrence by association falls into the latter category. By emphasising the most distinctive features of cyber space – that it has acquired universal value; that access to it is increasingly seen as a right; and that it is being encroached upon – deterrence by association offers the normative point of reference which has so far

been lacking in the cyber strategy debate, largely a result of the impasse caused by the attribution problem. Deterrence by association is a high risk strategy, politically and diplomatically, but it can establish the ground rules of a strategic relationship which can then develop into a policy of containment, if necessary, or engagement if possible through the digital equivalent of détente. ■

Professor Paul Cornish is Professor of International Security at the University of Bath. He was educated at the University of St Andrews (modern history), the London School of Economics (international relations) and received his Ph.D. from the University of Cambridge. He is a member of the UK Chief of the Defense Staff’s Strategic Advisory Panel, and has contributed to a number of Parliamentary inquiries and is a frequent commentator in national and international media.

REFERENCES AND NOTES

- ¹ Irving Lachow, “Cyber Terrorism: Menace or Myth?” in F.D. Kramer, S.H. Starr and L.K. Wentz, *Cyberpower and National Security* (Washington, D.C.: NDU Press & Potomac Books, 2010), p.440.
- ² Symantec Corporation, *Internet Security Threat Report* (Volume 16, April 2011), p.6.
https://www4.symantec.com/mktginfo/downloads/21182883_GA_REPORT_ISTR_Main-Report_04-11_HI-RES.pdf
- ³ “Danger: hackers at work,” *The Guardian*, 17 June 2011.
- ⁴ R. Clarke, “Obama’s Challenge in Cyberspace,” *Huffington Post* (www.huffingtonpost.com), 8 May 2009.
- ⁵ “Dyson: China has spy bugs in UK universities,” *The Sunday Times*, 27 March 2011.
- ⁶ “Embassy: Dyson spy claim is groundless,” *China Daily*, 6 April 2011, www.chinadaily.com.cn/cndy/2011-04/06/content_12276301.htm accessed 27 April 2011.
- ⁷ “China is accused of five-year cyber attack,” *The Daily Telegraph*, 4 August 2011. For the full report see D. Alperovitch, *Revealed: Operation Shady RAT* (McAfee, August 2011), <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>
- ⁸ J. Markoff and A.E. Kramer, “U.S. and Russia Differ on a Treaty for Cyberspace,” *The New York Times*, 28 June 2009: www.nytimes.com/2009/06/28/world/28cyber.html
- ⁹ “MoD under daily cyber attack, says Fox,” *The Daily Telegraph*, 8 June 2011.
- ¹⁰ “China and Britain locked in cyber war,” *The Telegraph* (www.telegraph.co.uk), 24 June 2011. See also “Chinese steal jet secrets from BAE,” *Sunday Times*, 11 March 2012.



REFERENCES AND NOTES

- ¹¹ “Foreign hackers putting UK firms out of business,” *The Daily Telegraph*, 24 October 2011.
- ¹² M. Hytha, “China-Based Hacking of 760 Companies Shows Global Cyber War,” *Business Week*, 13 December 2011: <http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html>
- ¹³ Office of the Director of National Intelligence, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Economic Espionage, 2009-2011* (Washington, D.C.: Office of the National Counterintelligence Executive, October 2011), p.1.
- ¹⁴ R. Bejtlich, *Tao Security* (blog), http://taosecurity.blogspot.com/2011/03/experts-talk-us-china-security-issues_07.html.
- ¹⁵ “The fourth modernization,” *The Economist*, “Friend or foe? A special report on China’s place in the world”, 4 December 2010, p.7.
- ¹⁶ Joseph S. Nye, “Nuclear Lessons for Cyber Security?” *Strategic Studies Quarterly* (Winter 2011), p.31.
- ¹⁷ A. Segal, “Is China a Paper Tiger in Cyberspace?” Council on Foreign Relations (blog), 8 February 2012: http://blogs.cfr.org/asia/2012/02/08/is-china-a-paper-tiger-in-cyberspace/?cid=soc-Facebook-in-China-paper_tiger-020812
- ¹⁸ A. Etzioni. “China: Making an adversary,” *International Politics* (Vol. 48, No. 6), p.648.
- ¹⁹ This section is drawn from P. Cornish, *Chinese Cyber Espionage: Confrontation or Co-operation?* (Bath: Cityforum Ltd, April 2012): <https://www.cityforum.co.uk/publications.asp>
- ²⁰ “Cyber Combat: Act of War,” *The Wall Street Journal* (Online), 30 May 2011: <http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html>
- ²¹ “Active cyber defence” is defined by the U.S. Department of Defense as synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities”: *Department of Defense Strategy for Operating in Cyberspace* (Washington, D.C., July 2011), p.7.
- ²² For a study of government/private sector relations in the United Kingdom see P. Cornish, D. Livingstone, D. Clemente and C. Yorke, *Cyber Security and the UK’s Critical National Infrastructure* (London: Chatham House, September 2011).
- ²³ See “Industry will have key role in U.S. cyber-security drive,” *Oxford Analytica Global Strategic Analysis*, 21 July 2011. For a European Union perspective see A. Klimburg and H. Tirmaa-Klaar, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU* (Brussels: European Parliament, April 2011), p.41.
- ²⁴ P. Cornish, R. Hughes and D. Livingston, *Cyberspace and the National Security of the United Kingdom: Threats and Responses* (London: Chatham House, 2009), p. 13.
- ²⁵ A. Blum, *Tubes: Behind the Scenes at the Internet* (London: Viking, 2012), p.5.
- ²⁶ “Commons” is defined in the *Oxford English Dictionary* as “provisions for a community or company in common”.
- ²⁷ A. Segal, “Can you hear me now? The U.S. sends China a message on cyber espionage,” Council on Foreign Relations (blog), 13 December 2011: <http://blogs.cfr.org/asia/2011/12/13/can-you-hear-me-now-the-u-s-sends-china-a-message-on-cyber-espionage/>
- ²⁸ P. Cornish, “Arms control tomorrow: the challenge of nuclear weapons in the twenty-first century” in R. Niblett (ed.), *America and a Changed World: A Question of Leadership* (London: Wiley-Blackwell/Chatham House, 2010), pp.232-233.
- ²⁹ Etzioni. “China: Making an adversary,” p.649.



Social Motivations in a Cyber World

— BY CLAIR STROM and MONICA AMARELO

The Internet era, like the Renaissance and Enlightenment before it, is one of the greatest revolutions to advance the potential of human achievement and human connection. Technology changes our expectations of each other and social media channels like Facebook, Google, and Twitter have transformed modern life.

One of the world's most original thinkers on technology trends, Ben Hammersley¹ has worked as a war correspondent and technological innovator. He coined the term “podcasting” and is the British ambassador to East London Tech City, the British Silicon

Valley. Hammersley is paid to tell stories about the future in order to understand the present.

In the words of the science fiction author William Gibson, “the future is already here, just not evenly distributed.”²

According to Hammersley, Facebook, Twitter, and Google now define modern life in the West. A functioning Internet with freedom of speech, and a good connection to social networks is not only a sign of modernity, but of civilization itself. The Internet is the central platform for business, culture, and personal relationships — “where we live,

where we bank, where we meet, where we fall in love.” The Internet is the dominant platform for life in the 21st century.

In 1963, Intel co-founder Gordon Moore made a bold prediction, popularly known as Moore's Law.³ Moore's Law states that the number of transistors on a chip will double approximately every two years. This golden rule is a guiding principle and a springboard for technological advancement. For the same price the number of components on an integrated circuit will double. Or conversely, the same amount of computing power will halve in price every 12 – 18 months.

MOORE'S LAW

Moore's Law is the foundation for exciting new technological capabilities and improved energy efficiency. While Moore's Law is the fundamental driver of the semiconductor industry, what's even more important is what it delivers to the consumer. Advances in process technology and reductions in cost make computing devices accessible to an ever-increasing number of people worldwide, empowering innovations—from the smallest handheld devices to the largest cloud-based servers.

Understanding Moore's Law is the key to understanding the modern world. The evidence of Moore's Law is everywhere, embedded in devices millions of people use every day, such as personal computers and laptops, tablets, smart phones, cell phones, common household appliances, and consumer electronics—as well as inspiring, important technological innovations in automobiles, life-saving medical devices, and spacecrafts.

Moore's Law has many implications and it makes planning a real challenge. For example, when Apple released the iPhone 3Gs in June 2009,⁴ it was a magical device. Three years later this amazing technology is obso-

lete. The new iPhone 5 will be 128 or 256 times as powerful as the iPhone 3Gs. The possibility for that increase in power is the driving force behind the modern condition.

CYBER AND INTERNET LAWS

Policymakers write technology laws that won't come into force for another couple years—by which time the technology won't exist anymore. Policies, therefore, need to be written with the future in mind.

10 – 20 years, enacting its rules on technology, which can't possibly yet be imagined. Policies, therefore, need to be written with the future in mind, not the present.⁵

Courts around the world also are creating Internet law right now—a process that is both exciting and frightening to watch. Unlike other areas of commerce that can turn to historical traditions to help settle disputes and guide the development of the law, the law of the Internet has no history to fall back on. Cyber law is being developed

For politicians it makes life very difficult. In terms of cyber security policy, officials are writing legislation for outdated technology. Today policymakers attempt to make laws to govern technology which won't come into force for another few years—by which time the technology won't exist anymore. These laws will be in force for the next

by judges who work to fit legal disputes on the Internet into preexisting frameworks. As a result, the legal principles governing conduct and commerce in cyberspace are in a state of flux. Claims of trademark and copyright infringement have become commonplace items on the world wide web.

For example, the 1996 Telecommunications Act,⁶ was relevant when passed but now is severely outdated since it only pertains to wired services and does not address wireless networks.

Two more recent examples are the Stop Online Piracy Act (SOPA)⁷ “to promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property, and for other purposes”⁸ and the Protect IP Act (PIPA),⁹ which started off in the U.S. Senate as the failed Combating Online Infringement and Counterfeits Act (COICA) from 2010.

Congress shelved both antipiracy bills¹⁰ indefinitely after Internet giants Google, Facebook, and Wikipedia rallied the world wide web to deal a major defeat to the traditional media industry while emboldening a new breed of online political activists. Congressional aides and lobbyists said lawmakers were reluctant to brave another firestorm incited by Google, Facebook, Twitter, Wikipedia and other popular websites during an election year.

CHANGING NORMS

The halving again and again of the price of technologies also is a problem for national security and defense. The general trend of technology moving forward means dangerous technologies are increasingly available to everybody and will inevitably become available to anybody with a credit card and an Internet connection.



As every aspect of our lives moves onto the Internet,¹¹ the need for robust security measures is great, but those security measures come with their own risks. What are we protecting, if the protection itself means we become, in some small way, a police state?

Under current defense philosophies, technological innovation inevitably leads to a constant state of asymmetric warfare. A new philosophy is required to reflect the present conditions and the future societal norms.

Telephone numbers are one example of a new norm. Before the turn of the century, a phone number represented a place—a house, an office, a booth – and the understanding that someone might not be at that place when a call was placed. Today, a phone number is a person. The switch in the meaning of phone numbers, from place to person, has completely changed social behavior.

In about ten short years, society has transformed from a specialist class of people with expertise to voice opinions to a reputation society.¹² In the past, verdicts on meals, books, music, television, films, products and politics were only shared

with a few people –neighbors, friends, and family. Today people assume that every meal, every hotel, every piece of culture consumed is something to have an opinion on and to share that viewpoint on the Internet. Today the Internet provides a place to review everything.

Twelve years ago, the only opinion that mattered was of the professional critic's. For example, to review a book, it was necessary to gain years of experience to become an authority. Today people are encouraged to submit reviews regardless of background or expertise.

The change in expectation causes problems, especially in the political arena. People write and post opinions in support of candidates and issues during elections. After a candidate is elected, those previously valued opinions no longer matter and are simply ignored.

In this way, society is renegotiating its social contract. The Internet, and the content on it, empowers people. People have become more sophisticated in their understanding of media and understand the value of data.

This leads to the next big social change. There is a growing expectation of

being able to access all the other data in the world and it actively changes the way people live. Digital natives will soon be in positions of authority, eager to take advantage of proliferating modes of global communication. In an age of proliferating data, smart phones and Internet literacy, we must remain aware that extremist messaging will reach more susceptible and receptive audiences than at any time in the past. ■

Clair Storm is a biomedical engineering student with a pre-law minor at Stevens Institute of Technology in Hoboken, NJ. Her research includes constitutional law and policy, political science, and judicial processes. During the summer of 2012, she studied law and public policy at Georgetown University and interned at the Federation of American Scientists.

Monica Amarelo is the managing editor of the FAS Public Interest Report and director of communications at the Federation of American Scientists.

REFERENCES AND NOTES

¹ Articles and biographical information on Ben Hammersley, editor-at-large of *Wired*: <http://www.benhammersley.com/>

² Wikipedia, the free encyclopedia, entry on William Ford Gibson: http://en.wikipedia.org/wiki/William_Gibson

³ *PC Magazine*, Encyclopedia, definition of Moore's Law: http://www.pcmag.com/encyclopedia_term/0,2542,t=Moore's+law&ci=47229,00.asp

⁴ Wikipedia, the free encyclopedia, entry on the technical specifications of the iPhone 3Gs by Apple Corporation: http://en.wikipedia.org/wiki/IPhone_3GS

⁵ The Internet Society provides this guide on Internet law as a public service. The guide provides links to many useful legal research sites on the Internet: <http://www.isoc.org/internet/law/>

⁶ Federal Communications Commission website. The Telecommunications Act of 1996 with text and links to additional resources: <http://transition.fcc.gov/telecom.html>

⁷ Wikipedia, the free encyclopedia, entry on the Stop Online Piracy Act: http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act

⁸ H.R. 3261 Stop Online Piracy Act, 112th Congress, House Judiciary Committee; October 26, 2011.

⁹ Wikipedia, the free encyclopedia, entry on the Protect IP Act: http://en.wikipedia.org/wiki/PROTECT_IP_Act

¹⁰ Jared Newman, *PC World*, "Congress Puts SOPA, PIPA on Hold," January 20, 2012: http://www.pcworld.com/article/248468/congress_puts_sopa_pipa_on_hold.html

¹¹ Congressional Research Service Report, "Promoting Global Internet Freedom: Policy and Technology," August 30, 2012: <http://www.fas.org/sfp/crs/row/R41837.pdf>

¹² Hassan Masum, Mark Tovey with foreword by Craig Newmark. *The Reputation Society - How Online Opinions Are Reshaping the Offline World*, MIT Press, February 2012: <http://mitpress.mit.edu/catalog/item/default.asp?tttype=2&tid=12750>

Nuclear Power Safety: Lessons From Three Mile Island and the Fukushima Reactor Accidents

ALEXANDER DEVOLPI *

ABSTRACT

Of accidents that have involved nuclear-power reactors, all have ultimately delivered useful lessons about nuclear safety, reactor design, and radiation effects. Despite three major mishaps at nuclear-power reactors (in the United States, the former Soviet Union, and Japan), the accidents are noteworthy for very few, if any, public casualties. However, psychological trauma shocked the industrial world, and their occurrence has had expensive consequences in terms of radiation cleanup, power loss, decommissioning, and public apprehension. Now three Fukushima Daiichi reactors remain at risk of further internal damage. Irrespective of each deplorable accident, nuclear safety has duly improved, and important functional lessons have been derived.

Nevertheless, more could have been and could yet be implemented from the experiences, including added measures to diminish reoccurrences and consequences. In particular, a fundamental instrumentation shortcoming that contributed to the Pennsylvania Three Mile Island (TMI)-2 reactor meltdown was never fully addressed, and that omission might have indirectly hastened Fukushima reactor damage. Also yet to be implemented are some remedial measures and precautions forestalling the brutal hazards of further Fukushima fuel meltdown and subsequent reactor decommissioning.

This article (with supplementary sidebars) describes some overlooked autonomous nuclear instrumentation that can be installed to independently measure reactor water level and fissile fuel distribution — before, during, and after an accident.

MAJOR NUCLEAR REACTOR ACCIDENTS

Three accidents of significant consequence have occurred among civilian nuclear power reactors: TMI-2 in Pennsylvania (1979); Chernobyl in the former Soviet Union (1986); and Fukushima in Japan (2011).

Although these accidents resulted in devastation of the reactors, none caused provable injuries to members of the public. That judgment may startle many readers, but it is a demonstrably valid conclusion to draw from the various international technical assessments.

First of all, it's well-substantiated that neither the TMI nor Fukushima accidents have been

responsible for any fatalities to date among the surrounding public. As for the Chernobyl nuclear-reactor destruction, it directly led to about three dozen deaths among operators and emergency workers, according to international Chernobyl Forum study reports that have tracked mortality data since the accident. With regard to potential fatalities induced by Chernobyl radiation fallout, no provable morbidity has been observed in the affected territories, even a quarter of a century later, contrary to dissenting predictions based on theoretical expectations. An international Chernobyl Forum report, 25 years after the accident, projected up to 4000 premature public fatalities, but there has been no actual post-mortem body count to validate that statistical estimate.



While (theoretically) a small percentage of thyroid cancers among juveniles might be attributable to the added radiation, it is surpassed by many more similar occurrences resulting from health-care deficiencies in the former Soviet Union. The Chernobyl Forum estimated about 15 radiation-induced thyroid-cancer fatalities, about one hundredth of the number of relevant juvenile deaths resulting from chronically poor medical treatment.

No matter what the actual incidence of human fatalities, considerable motivation exists to improve nuclear-reactor safety, at the very least because of financial impact, psychological trauma, and electrical capacity loss. Despite such long-standing incentives, some worthy engineering improvements have not been implemented for commercial reactors.

The TMI and Fukushima installations suffered accidental loss of water needed to remove residual heat from the reactor. This sudden coolant deficit resulted in serious damage to overheated nuclear fuel within the central (core) region.

I've had 40 years of technical education and experience in the nuclear field. My considered evaluation is that the disastrous TMI meltdown could have been averted if reactor operators had been aware that coolant in the nuclear core was below the level and density needed for heat removal.

Unanticipated conditions had degraded the TMI emergency cooling system, and existing conventional water-level indicators failed to function properly or meaningfully; thus, the amount and density of coolant water in the reactor vessel was not available to trained operators in the control room.

Had actual (insufficient) coolant conditions been known to the reactor operators, the entire TMI core meltdown would likely have been prevented.

And, as for the three Fukushima reactors, if the operators implemented (or had been able to implement) extraordinary emergency cooling measures sooner, they too might very well have forestalled or mitigated reactor-core damage.

The lead title of this paper was chosen deliberately to emphasize the safety of commercial nuclear power, thus alluding to the central function and necessity of water-

transported heat, a role just as important as a controlled nuclear reaction.

Nevertheless, despite the occurrence of several major power-reactor accidents, no autonomous means of measuring water-coolant levels has been installed in commercial reactors.

Damaged reactors must be gradually and safely shepherded into a condition known as "cold shutdown" being disassembled and decommissioned. For TMI, the post-accident stage required about ten years. It involved substantial effort and cost, as well as the development of special decommissioning technologies. For the disabled Fukushima reactors — in order to better assist their harmless, systematic, and expeditious stabilization and dismantlement — it would be wise to anticipate and implement technical measures based on the TMI experience.

This article, and accompanying sidebars, contains my professional interpretation of some crucial events that led to core meltdowns at TMI and Fukushima.

CIRCUMSTANCES OF THE TMI REACTOR ACCIDENT

Two reactors were built in the 1970s on Three Mile Island in the Susquehanna River near Harrisburg, Pennsylvania. Both were of the pressurized-water type manufactured by the Babcock and Wilcox Company. In 1968 construction began on TMI-1, which commenced operation in 1974; it has now operated without incident for over 38 years. The second reactor suffered its ill-fated accident after just one year of operation.

The accident at TMI-2 was precipitated when a relatively minor malfunction in fluid flow caused its primary coolant temperature to rise. This in turn compelled the reactor to shut down automatically in about one second. A pressure-relief valve then failed to properly shut, but control-room instrumentation did not reveal that closure. As a result, coolant drained from the reactor core, and residual nuclear-decay heat was not removed at a sufficient rate. Worse yet, the reactor operators — erroneously believing at the time that there was too much water in the pressure vessel — turned off the emergency core-cooling system,

and — after an hour or so of unrecognized overheating — they closed down the coolant pumps, further aggravating the situation.

During the accident sequence, operators and supervisors were unable to diagnose or respond properly to the unplanned automatic reactor shutdown. More specifically and more constraining, they did not have real-time knowledge of how much coolant water was in the reactor vessel, nor did they have any information about fluid density while the accident transpired. They had no actionable indication that coolant capacity was insufficient to relieve the dangerous overheating of reactor fuel.

Whereas instrumentation for monitoring and managing the fission-induced *nuclear* reaction functioned properly, the internal means to regulate water-transported *power* production failed, and no autonomous auxiliary indicators were available to alert operators of the impending disaster.

Evaluating the Accident

Major government and industry studies and evaluations ensued. Root causes of the TMI accident were ascribed largely to deficient control-room instrumentation and to inadequate emergency-response operator training. In addition, critical human factors and user-interface engineering problems were identified.

While unanticipated conditions did occur, some relevant conventional instrumentation inside the reactor failed to function. According to the World Nuclear Association, no direct information was available to the operators during evolution of the accident regarding the amount of water actually in the reactor vessel.

Lacking direct water instrumentation, control-room operators judged coolant solely by the pressurizer indicator, which advised that water level was apparently high. Thus, the operators assumed the core was properly covered with coolant, unaware that steam in the reactor vessel provided misleading pressure readings. This was a key contributor in their initial failure to recognize loss of coolant.

Had the operators known that water was being lost from the reactor vessel (and the core was going without coolant), the destructive part of the accident could have been avoided by correct remedial actions. As best as I can find, that conclusion never became actionable or even noticeable in subsequent commissioned reports or official follow-up dockets.

Aside from the traumatic accident event itself, the condition of the self-destroyed reactor remained for many years in a state of devastation and uncertainty. Nearly 10 years went by before it was confirmed that half the core fuel had melted and settled in the bottom of the pressure vessel.

What Lessons Were or Were Not Implemented?

Of the several comprehensive investigations that followed, the most influential was that conducted by the Kemeny Commission appointed by President Carter. It resulted in many recommendations, most of which were followed. For example, improvements were advised and implemented in procedural and analytical areas: operator training, emergency planning, dissemination of industry information, use of probabilistic safety assessment, and analysis of likely events.



Within the narrow purview of this article on major reactor mishaps, here's my own emphasis on relevant events that took place during the TMI accident:

- (1) Existing conventional reactor instruments failed to reveal the ongoing loss of coolant. Because internal water and pressure sensors were gradually destroyed in the course of the accident, they were unable to supply critical information for the grave situation that evolved.
- (2) Although there were some external instruments were on the reactor bridge structure outside the pressure vessel, those devices could not and did not help diagnose the loss-of-coolant evolution.

Notably absent from official post-TMI reports was a recommendation to implement autonomous external water-level instrumentation. Such specialized equipment, based fundamentally on nuclear rather than conventional sensor principles, would operate in such a manner as to be functionally and physically independent of other instruments and their power sources.

Whereas TMI operators had to infer the actual loss of coolant from an array of contradictory indicators, an instrument which directly measured reactor water level would have provided definitive information that reasonably might be expected to have prevented the reactor meltdown. This is what led me to applying 20 years of instrumentation experience toward devising and patenting a method for autonomous real-time detection of water level and density.

Had such an independent water-level diagnostic monitor been in operation, unambiguous loss-of-coolant data should have been available to reactor operators; therefore, subsequent core meltdown might very well have been averted. There would then have been clear indication that the water volume and density were actually being reduced rather than sustained during the accident sequence.

Although other measures to prevent or mitigate the same type of accident have since been taken in the 30 or more years after the TMI event, no operating nuclear reactors have been retrofitted with failure-resistant water-level instrumentation positioned external to the pressure vessel.

CIRCUMSTANCES OF THE FUKUSHIMA REACTOR ACCIDENTS

The extraordinary 11 March 2011 Tohoku earthquake of estimated 9.0 magnitude off the coast of Japan not only caused severe damage to populated areas, it also induced a

tsunami that breached protective seawalls. Up to 20,000 residents are known to have died; 125,000 or more buildings were damaged or destroyed; and there were a multiplicity of secondary effects, such as nuclear-plant shutdowns and meltdown accidents near the earthquake epicenter. The unprecedented tsunami overwhelmed ocean-facing barriers at the Fukushima Daiichi nuclear-power station, thereby flooding subterranean backup power generators and pumps.

Although all Fukushima reactors had promptly shut down when the earthquake struck, the floods led to interruption in normal coolant-water recirculation. That was one of several nearly simultaneous consequences of the earthquake-induced electric-grid failure. Emergency electrical generators came on line for electronic controls and coolant systems, but backup electrical supply was insufficient for the reactor pumping systems. Moreover, reserve fuel for emergency generators was not intended to last more than about a day.

Some factors that caused internal reactor damage were similar to the accident at TMI in the sense that (1) the hot reactor core was suddenly deprived of sufficient water coolant, and (2) *ad-hoc* measures had to be undertaken to provide emergency cooling. At the Fukushima nuclear station, the contrived remedial measures, including injection of ocean water, were not sufficient to prevent partial or full core meltdown in the three reactors that had been in operation.

The Fukushima Dai-ichi nuclear power station is comprised of six separate boiling water reactors originally designed by General Electric and maintained by the owner-operator, Tokyo Electric Power Company (TEPCO). Combined electrical power for the station was 4.7 GWe. At the time of the quake, Reactor 4 had been de-fueled, while units 5 and 6 were in scheduled cold shutdown for planned maintenance. Before the earthquake, Units 1 to 3 were providing power at rated output.

After the earthquake, control rods were inserted, and the operating reactors (marked 1, 2, and 3 in Figure 3) automatically scrammed (closed down). When external electricity was lost, emergency diesel generators started up properly and many other instruments also functioned as designed.

About an hour later, the tsunami not only broke connection to the power grid, it also resulted in flooding of sub-grade rooms containing emergency generators. Consequently those generators stopped working and pumps that circulate coolant water in the reactor ceased to work, causing the reactors to start overheating. Operators were still engaged in prescribed post-shutdown procedures, such as controlling reactor pressure with limitations not to exceed an established cool-down rate. The flooding and earthquake damage greatly hindered external assistance.

Unanticipated site flooding resulted in impairment of electrical backup systems that would have sustained the Fukushima reactors during a safe, controlled shutdown. Flooding also led to failure of secondary systems and to

dramatically destructive explosions in three reactor buildings. Volatile gases had originated inside the reactors after zirconium fuel cladding reacted chemically with coolant water to produce a buildup of explosive hydrogen. In addition, radiation escaped reactor containment, polluting the land, sea, and air environment — although no known human casualties are known to have resulted, and it is not likely that any will occur.

Because of the tsunami, AC power sources (except for one emergency diesel generator) lost their functions, and motor-driven pumps and valves were inoperable. Numerous switch gears were wet or flooded and becoming unusable. Units 1, 2 and 4 lost their DC sources, resulting in monitoring instruments being put out of use. Backup seawater facilities necessary for heat removal from reactors had also been flooded; this resulted in inoperability of large pumps and other equipment that required cooling of motors.

Immediately after the tsunami, steam-driven pumps, such as the core-isolation cooling system, were used to inject water into the reactors; these pumps eventually stopped working. Because water injection into the reactor was essential to cool the reactors, depressurization of the pressure containment vessel was unavoidable. Since no power sources were available in order to operate valves, workers had to conduct or devise alternatives; for example, they used car batteries. Preparations for venting were implemented using temporary equipment under harsh conditions after such startling events as the hydrogen explosions.

In short, destruction caused by the tsunami resulted in loss of almost all equipment and power-source functions expected to be activated in case of accidents, including those for accident-management measures. Workers on the site were forced to adapt to sudden changes of circumstances, such as injecting water into the reactors using fire engines, and accident management became extremely difficult.

When AC and DC power failed, no staged emergency equipment was available for injecting cooling water into the reactors. The unavailable functions included steam-driven high-pressure water-injection systems and motor-driven cooling facilities. Instead, fire-protection lines (originally prepared for accident management) were utilized used to inject water. The work was made very difficult due to scattered debris caused by the tsunami, by lack of suitable lighting, and by frequent earthquake aftershocks. Fresh-water injection commenced early in the morning of March 12. Work conditions further deteriorated due to increased on-site radiation levels and the hydrogen explosions. The extraordinary measure of injecting seawater started in the evening of March 12.

An outside review of the accident progression, adapted from a report prepared by an international organization of experienced nuclear plant operators, is presented in a sidebar.

Tenuous Post-Accident Situation

The current condition of Fukushima Units 1, 2, and 3 is relatively static, but those reactors have yet to achieve a stable, cold shutdown. This means that they could still undergo various and uncharted stages of self-destructive disassembly and meltdown.

More than a year after the core meltdowns, the affected reactors remain in uncertain conditions that could still benefit from diagnostic information specific to (1) their existing, but unknown, post-accident coolant level, (2) the current status of undetermined core redistribution, and (3) any other changes that might yet take place in time. The responsible managers simply don't know how much water is in the pressure vessels, nor do they know where the nuclear fuel is now located.

Despite the meltdowns, no known reactor-related fatalities were caused among members of the public or among nuclear workers; however, substantial loss of electric power and economic value has resulted. Moreover, it will take many years or decades to decommission the nuclear reactors in a harmless and systematic manner.

Current estimates of the total earthquake- and tsunami-related economic costs are well over \$200 billion, not including tens of billions of dollars attributable to decommissioning and the loss of power from the disabled reactors.

Figure 4 contains a graphic rendition of the typical Fukushima reactor building profile, with callouts for the overhead fuel storage pool, the reactor pressure vessel (RPV), the reactor core, the concrete biological shield, and the 67-foot diameter reactor pressure-containment vessel (PCV) inside the biological shield.

The reactor water level in Fukushima Unit 1 is considered to have receded within a short period of time, leading to exposure of the reactor core and to core damage. Reactor pressure decreased even though no actions were taken to reduce it. On the other hand, PCV pressure increased, implying that reactor-vessel pressure could not be maintained due to stresses on the vessel, and that the core damage had advanced a considerable extent within a short period of time.

For Units 2 and 3, reactor water level started to decrease after cooling circulation stopped. Fire-engine pumps were started and low-pressure water injection was ready, but it couldn't be started quickly enough. The amount of water in the reactors sharply decreased. This resulted in core damage, for Unit 2 about two hours after the earthquake, and for Unit 3 in about 60 hours.

Because of the extraordinary conditions, boric acid and seawater were injected into the unsalvageable reactors in order to quench possible nuclear recriticality.

Remaining Uncertainty About Damaged Reactors

Despite adept and courageous efforts by qualified TEPCO personnel, risk remains of potentially harmful degradation of the reactors at the Fukushima power station. Although nominally out of operation, three of the reactors are not in a consummated state of managed control known as “cold shutdown.” Even a year later, each generates many megawatts of heat and radiation.

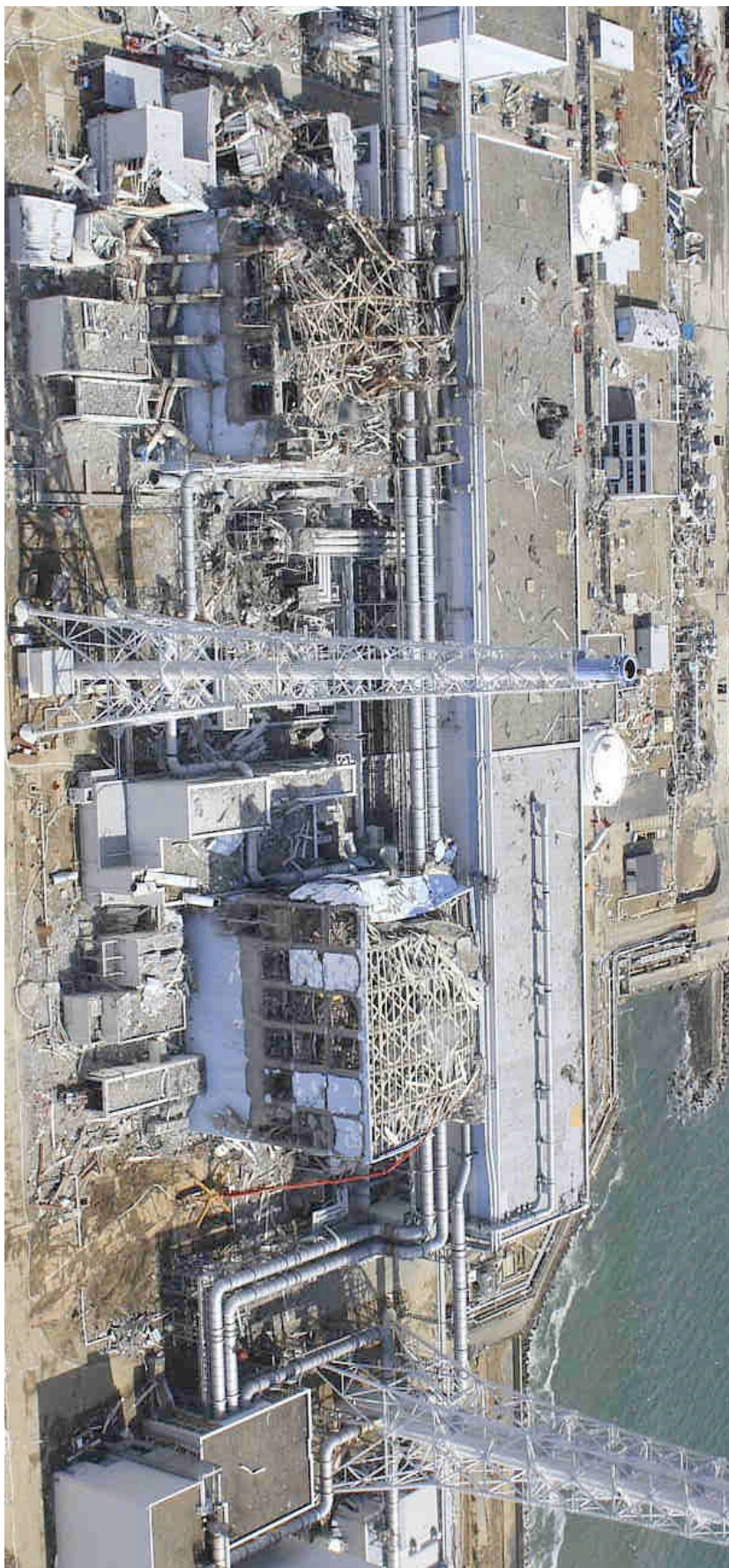
Before decommissioning can take place, TEPCO will have to manage and control a difficult situation that presents technical and public uncertainty.

Most uncertain is the ongoing condition of the nuclear core and its water coolant — a continuously changing and currently indeterminate situation. Because normal water supply was interrupted by failure of electrical pumps and other emergency measures, extraordinary methods are currently being used to supply sufficient water coolant for the three damaged reactor vessels. In fact, forced external cooling will probably be necessary for many years.

In addition, nuclear fuel in one or more of the reactor cores has been damaged, likely to have been partially or fully melted, such that some or much core material fell to the bottom of their pressure or containment vessels. This problem is compounded because of the small, but finite possibility of “recriticality” in which a reactor might spontaneously renew production of a fission chain reaction that cannot be properly cooled or safely contained. Such nightmarish scenarios are more conceptual than realistic, but properly informed measures are needed to cool, control, and manage the residual nuclear-reactor cores until fully decommissioned.

Getting the disabled Fukushima reactors decommissioned in a safe, timely, and orderly manner is a common goal of public, professional, and international concern. Meanwhile, three reactors remain in a tenuous condition that could yet lead to additional hazardous consequences and public alarm.

In this March 24, 2011 aerial photo taken by a small unmanned drone and released by AIR PHOTO SERVICE, damaged Unit 3, left, and Unit 4 of the crippled Fukushima Dai-ichi nuclear power plant are seen in Okumamachi, Fukushima prefecture, northern Japan. (Air Photo Service Co. Ltd., Japan)



EXPEDITING FUKUSHIMA REACTOR CLEANUP

When the Fukushima-reactor cleanup staff and crew is ready to plan and engage in removal of fuel and core debris, it would be extremely valuable, probably essential, to have updated knowledge of the approximate quantity and geometrical distribution of water and fuel inside the reactor pressure vessel. Such information would help safely and economically manage residual nuclear-criticality and radiation-exposure risks for each disabled reactor.

Based on the decade of TMI-2 field experience and costly delays in removing degraded fuel, it would be wise to consider supplementary diagnostic measures that might help expedite the cleanup at Fukushima.

External instrumentation could be introduced for the specific purpose of determining how much water is currently within the reactor vessels. That same external instrumentation, if based on measurement of penetrating radiation, could be used to map the physical arrangement of the intact and/or crumbled reactor fuel. Such information would be important in safe and methodical dismantlement, which might take up to ten years. Much of this is now cleverly being deduced from indirect instrument data and analysis.

An early step towards directly characterizing the redistributed core fuel could be achieved by introducing specialized instrumentation placed inside the reactor containment building — but outside the pressure vessel. To accomplish this, a modified “fast-neutron/gamma-ray hodoscope” diagnostic system could be installed and operated by remotely-controlled equipment (See technology sidebar). There are two manifestations of this instrumentation, depending on the degree and access available within or inside the biological shield. Of course, a major limiting factor will be safe and practical access to requisite areas inside the reactor building.

The technical term “hodoscope” applies here to a calibrated set of radiation-detecting instruments that differentiate the direction and energy of selected nuclear radiation. Fast neutrons and gamma rays are forms of penetrating radiation that originate inside nuclear reactors, whether operating at full power or closed down after a long history of operation, as at Fukushima. Residual radiation emerging from the now-inoperative reactors provides a way to measure the existing quantity and distribution of water and fuel in the reactor.

Considerable and relevant experience has been accumulated, used, and published that is relevant to this proposal. Information was obtained and analyzed from very reliable and successful hodoscope operations under severe

radiation conditions. The experience base is derived from 30 years of design, experiment, and operation.

Hodoscope-type systems could be installed and operated inside the biological shield, but external to the reactor pressure vessel of each disabled Fukushima reactor. The equipment would be expected to deliver information in real time on the reactor coolant and fuel distribution. These essential items of information are now highly uncertain at the fatally damaged reactors which might have fuel that has drained into the bottom of the containment vessel.

Because this diagnostic approach had been overlooked, its function is described here in some detail. The hodoscope system is based on the body of experience and concepts disclosed in patents detailed in the technology sidebar.

Improving Knowledge of Core and Coolant Condition

This particular external equipment was specifically conceptualized as a result of the 1979 TMI-2 nuclear accident in Pennsylvania, and it was formalized in a U.S. patent issued in 1987. (Had this instrument system already been installed at the TMI-2 reactor, it is likely that the traumatic billion-dollar accident could have been averted.)

Implementation at Fukushima can yet assist in preventing further damage by removing uncertainty regarding the ongoing nuclear-fuel condition and water-coolant status. If positioned beforehand, the diagnostic instrument system — designed to survive an accident of the type that occurred — would likely have remained functioning to provide post-accident real-time information on the status of coolant and fuel.

A conceivable alternative or complement to the stationary diagnostic coolant and fuel monitoring system would be a mobile array of collimated detectors. It would have to be positioned within the biological shield and reactor containment, but outside the reactor pressure vessel. Such a system could be remotely operated so as to provide crucial coolant and fuel profiles as needed.

For perspective, it should be recognized that — while the proposed diagnostic instrument system has a solid foundation in prior research, development, testing, and supportive calculations — it has not been actually assembled and tested in a water-cooled power reactor. An evaluation program is under consideration in the Nuclear Engineering Division of Argonne National Laboratory.

DISCUSSION AND CONCLUSIONS

One should ask, why — after the TMI accident — were there no high-level recommendations for external water and fuel monitoring? While major post-accident expert reports identified numerous errors and remedies — in TMI reactor design,



construction, and operation — no requirements seem to have been included for autonomous measurement of bulk water level.

In both the TMI and Fukushima accidents, incorrect operator response and poor control-room organization were major factors in either initiating or aggravating the respective incidents (along with many other contributing factors that have been duly recognized). Nonetheless, during these specific power-reactor emergencies, no direct data on actual coolant immersion or voiding in the core were available to the operators.

Belatedly, without authorizing relevant action, an official 2004 *NRC Fact Sheet on the Accident at Three Mile Island* acknowledged explicitly, “There was no instrument that showed the level of coolant in the core.”

Possible explanations for omitting autonomous bulk water monitoring are that such an objective was deemed technically too speculative, too difficult, or too intrusive to achieve.

Although the worldwide nuclear industry has implemented and touted higher levels of safety, reliability, and training in the operation of nuclear power plants, apparently little has been done to provide supplementary

external instrumentation.

Had such an innovation been mandated for the Fukushima reactors, it is plausible that their core meltdowns might have been averted or minimized because operators would have been better informed by direct measurement of ongoing loss of coolant.

It’s not too late for the disabled Fukushima reactors to benefit from *post-hoc* introduction of diagnostic monitoring equipment.

Nor is it too late to develop and test the proposed diagnostic system for a role in commercial power reactors throughout the world. Although a number of measures to prevent or mitigate the same type of accident have been taken in the 30-plus years since the TMI event, no operating nuclear reactors have been retrofitted with failure-resistant autonomous water-level instrumentation positioned external to the pressure vessel.

Of the three major accidents involving nuclear-power reactors, all have ultimately delivered useful lessons about nuclear safety, reactor design, and radiation effects. Moreover, those particular accidents are noteworthy for very few, if any, public casualties. Nevertheless, trauma from their occurrence has shocked the industrial world, while radiation cleanup,

power loss, and reactor decommissioning have been expensive. Despite such deplorable events, nuclear safety has duly improved, and important functional lessons have been derived. Even so, more can be learned from the experiences, including better instrumentation to diminish reoccurrences and consequences.

In the aftermath of the TMI nuclear meltdown, massive resources were unleashed in analyzing the accident and advising remedial actions. Many generic reactor improvements were undertaken, but — as indicated by the accident progression at Fukushima — one of the most conspicuous remedial actions to be derived from TMI was never implemented: No autonomous information on the reactor-core water level was available for the Fukushima operators, who erroneously inferred that water was surrounding the reactor fuel.

Several formal post-accident investigations extensively analyzed the TMI event. The Kemeny Commission attributed “operator error” as the decisive factor. Their rationale was that if reactor operators had not erroneously turned off emergency cooling systems, the accident would have been limited. But the operators had no direct indication that coolant water was turning into steam. If there had been in place a means of externally monitoring water level and density, it might have prevented the meltdown.

As best as I can tell, no autonomous water-level monitor has since been prioritized, mandated, or installed in any new reactor construction — despite the imposing array of TMI post-accident reviews, critiques, and interventions involving the Kemeny and Rogovin investigative boards, Nuclear Regulatory Commission follow-ups, Department of Energy government R&D, UK Chief Inspector, Babcock&Wilcox manufacturer improvements, and watchdog groups like the Union of Concerned Scientists.

The tsunami subjected the Fukushima reactors to chaotic conditions. If independent water-level instrumentation had been installed, there is at least a chance that earlier remedial actions based on contemporaneous knowledge of coolant

level might have been terminated the accident progression before core meltdown. Because instrument shortcomings at the TMI-2 reactor were never fully addressed, that unrecognized omission might have allowed Fukushima reactor-core damage to have been exacerbated. Even a very recent 2011/2012 NRC Task Force Review of Insights from the Fukushima Dai-ichi Accident failed to make recommendations dealing with the instrumentation highlighted in this paper.

My recommended autonomous instrumentation is designed to collect data years after a reactor has nominally ceased operation. At Fukushima, such supplementary nuclear instrumentation could still provide real-time post-accident monitoring of both water level and fuel distribution until the reactors are defueled.

TMI technical reviews do not seem to have adequately prioritized an essential mandate, namely that power-reactor water coolant is such a fundamental property that it should be directly monitored.

The brutal hazards from core meltdown and subsequent reactor decommissioning might further be minimized by some selected remedial measures and precautions that could be implemented. This article has outlined autonomous external nuclear instrumentation that can still be installed — at Fukushima and at operating power reactors — to independently measure reactor water level and fissile fuel distribution — before, during, and after a reactor accident or routine shutdown. ■

Dr. Alexander DeVolpi, a retired nuclear physicist, has almost 40 years of experience in reactor instrumentation, experimental diagnostics, and specialized technology at Argonne National Laboratory, near Chicago, Illinois. He has a PhD in physics, an MS in nuclear-engineering physics (both from Virginia Tech), and a BA in journalism (from Washington and Lee), as well as being a graduate of the International School of Nuclear Science and Engineering (at Argonne).



Technology Relevant to Important Reactor Properties

By Alexander DeVolpi

Here are descriptions of technology and patents relevant to determining how much water and fuel is in a nuclear reactor, whether the reactor is at full power or shutdown.

The basic patent relates to a device called a hodoscope, which has been designed and developed to measure the rate and direction of specific nuclear radiation. The other two patents are proposed hodoscope applications, the first one for use with operating light-water power reactors, and the second for the dysfunctional Fukushima reactors that are now closed down.

The diagnostic hodoscope device is well anchored by many years of experimental data and supplementary

calculations. It is intended to provide an autonomous means of determining water coolant level and the bulk fuel distribution in an operating nuclear-power reactor, even after the reactor has shut down.

These patents and their technology are thus relevant to the tenuous situation that now exists at Fukushima, and the patents also are applicable to other water-cooled nuclear reactors operating around the world. The first two patents have expired and are in the public domain, while the third was recently filed.

Basic Hodoscope Patent

The neutron/gamma hodoscope (1978

US patent 4,092,542, "High-Resolution Radiography by Means of a Hodoscope") is a diagnostic device that has succeeded in producing radiographic-type images of objects inside nuclear reactors under extremely difficult and unusual operational conditions.

In the accompanying block diagram (Figure 1), the neutron source and target would ordinarily be inside the core of the nuclear reactor, while the hodoscope multi-channel collimating and detecting apparatus would be installed within the reactor's biological shield, and the remainder of the data storage and electronic system would be outside the reactor shield.

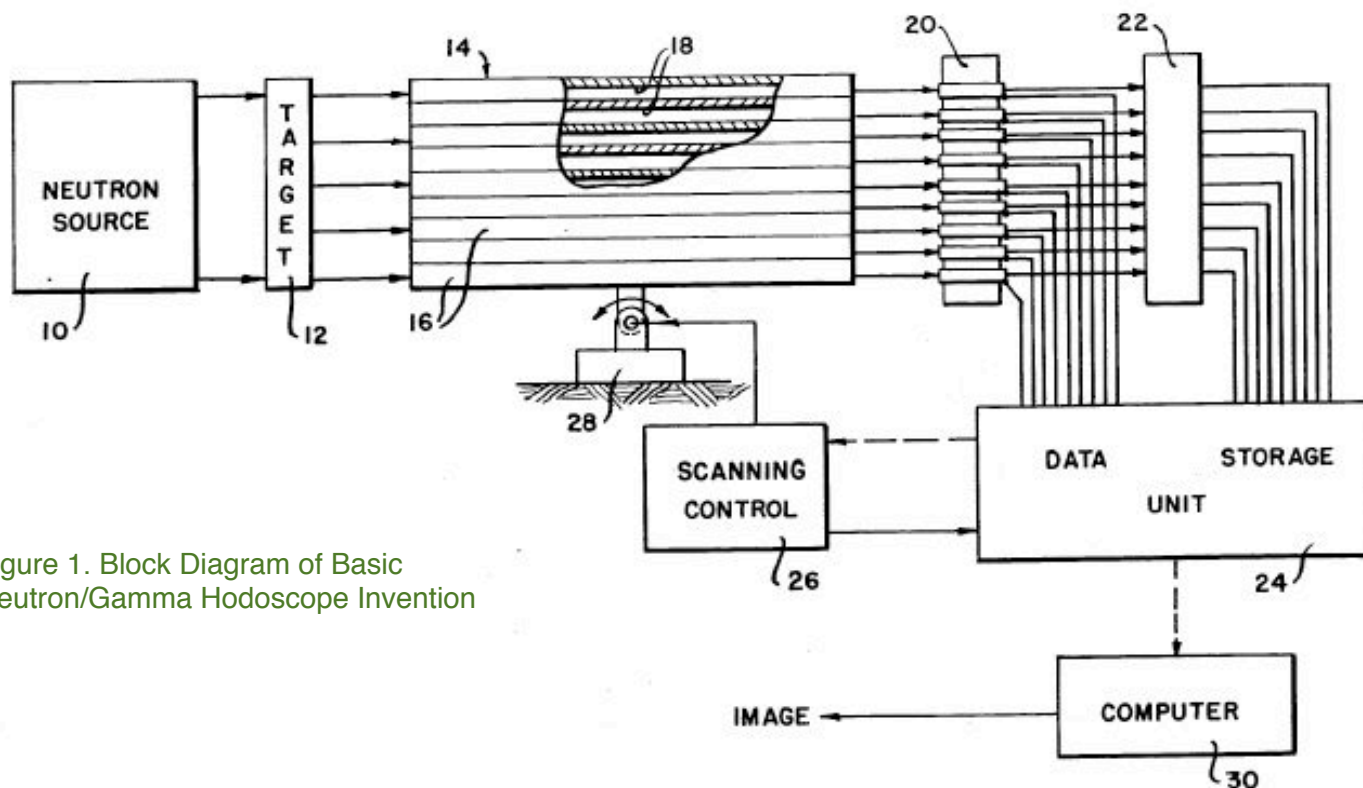


Figure 1. Block Diagram of Basic Neutron/Gamma Hodoscope Invention

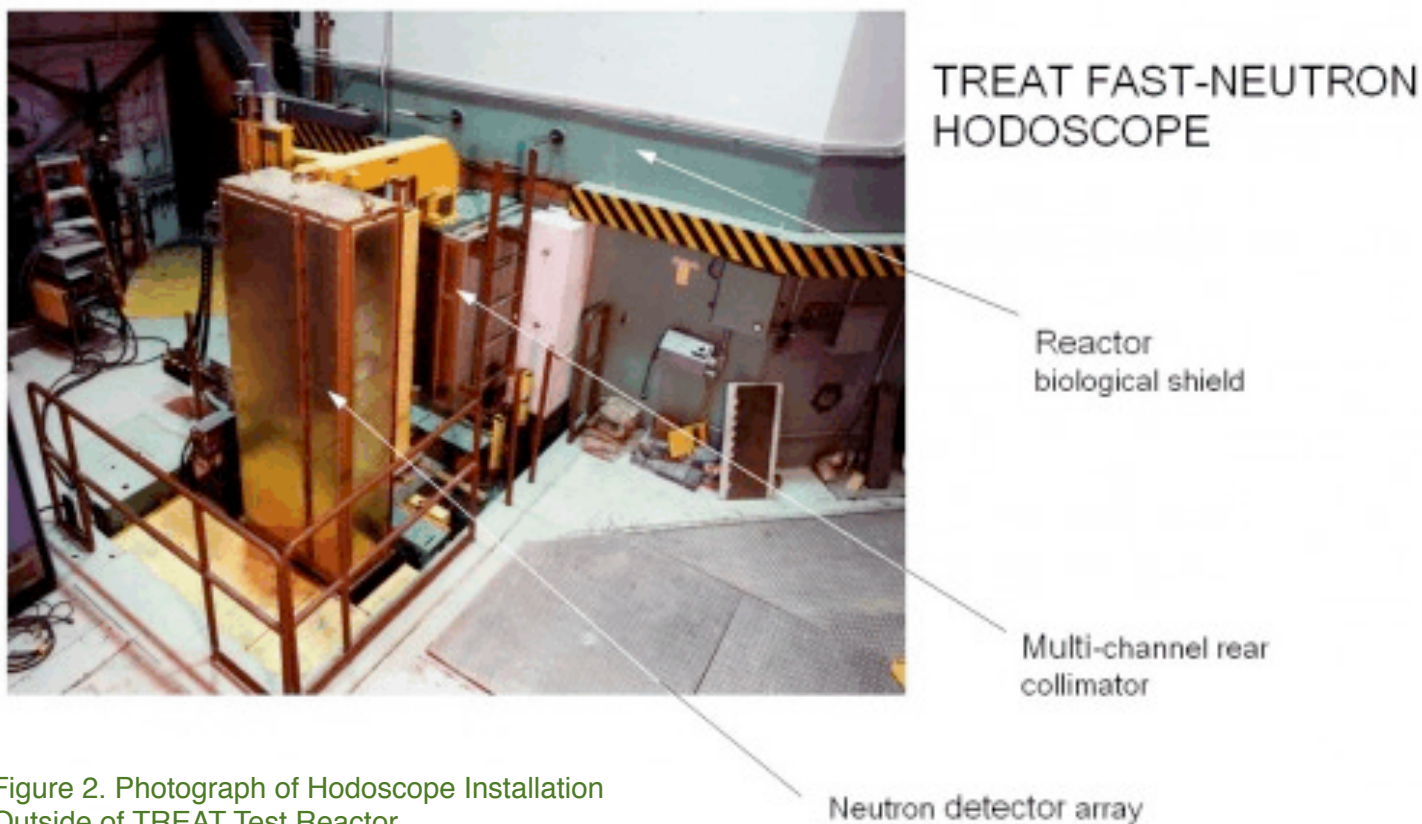


Figure 2. Photograph of Hodoscope Installation Outside of TREAT Test Reactor

The collimator might be installed several meters from the target, as shown in Figure 2, in which case the detectors are over 5 meters from the test element.

In the United States and France, hodoscopes have been installed in a similar manner outside or at the edge of nuclear reactors. The devices have rendered time-resolved image reconstructions of fuel and coolant that have been deliberately subjected to severe test conditions within the reactors.

Figure 3 shows a cross-sectional image of the hodoscope at the TREAT transient test reactor at the Idaho National Laboratory.

These diagnostic-radiation hodoscopes have also been used to geometrically characterize stationary objects irradiated by neutron and gamma sources inside reactors.

TMI-Inspired Hodoscope Patent

Stimulated explicitly by the 1979 loss-of-coolant accident at the TMI-2 reactor in Harrisburg, Pennsylvania, a patent (US 4,649,015, "Monitoring System for a Liquid-cooled Nuclear Fission Reactor," filed in 1984, was issued in 1987 (Figure 4).

This invention, based on substantial and relevant technical experience with the hodoscope, was intended to provide a physically and functionally independent (autonomous) means of monitoring downcomer, core, and plenum liquid levels in water-cooled nuclear reactors.

The reactor-radiation-driven measurement data could be collected in real time, as well as after the reactor was shut down.

The ultimate purpose was to provide an independent and durable means for minimizing real-time

operational uncertainties about water levels and steam conditions in a reactor. This would address problems that have already aggravated accidents in water-cooled reactors.

This patent was never implemented nor tested in a commercial power reactor — an important limitation that must be acknowledged. However, the design is supported by detailed numerical calculations, experiment-based computer modeling, and an extensive foundation of experimental data obtained under relevant conditions.

New Patent: Monitoring Fukushima Reactors With a Hodoscope

Taking note of unresolved similarities in both the TMI and Fukushima nuclear accidents, a provisional patent was filed this year: "Radiation-

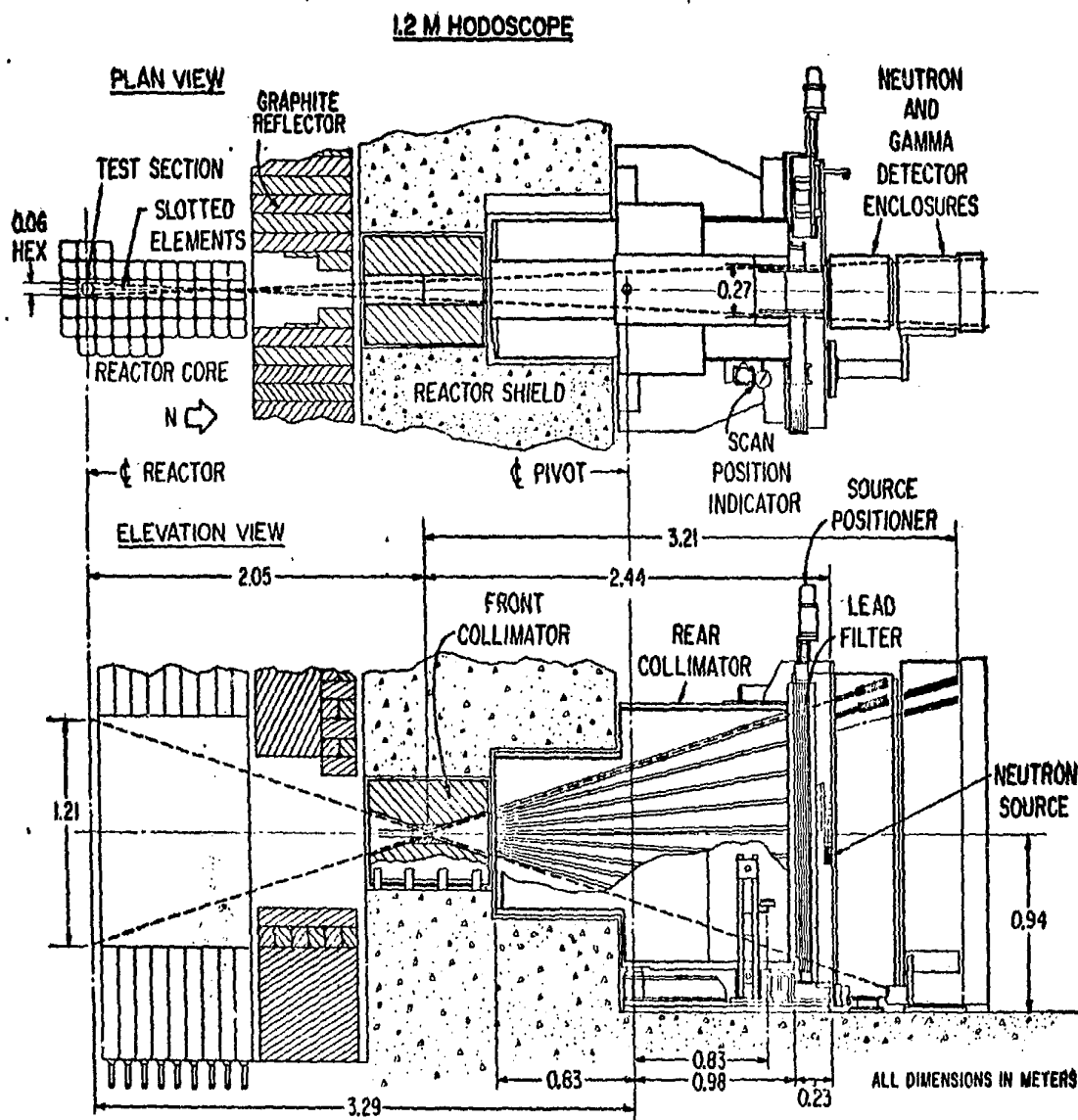


Figure 3.
Cross-Sectional
Top and Side
Views of Newer
Hodoscope at
TREAT

Fig. 3. Schematic diagram of hodoscope

Monitoring Diagnostic Hodoscope for Fukushima Reactors.”

The objective is to instrument the Fukushima reactors with autonomous remotely-operated radiation sensors located inside the reactor biological shield. In this manner, it would be possible to safely monitor the water and fuel now inside the pressure or containment vessel. Having definitive knowledge of water level and nuclear-fuel distribution is crucial for the safe and timely decommissioning of disabled reactors.

There are two manifestations of this invention: One provides for permanent detector array installation by means of narrow penetrations through the reactor biological shield. The other manifestation offers a mobile detector array that might be emplaced and operated by robotic means inside the biological shield.

Extrapolating from the decades of experience with radiation-detecting hodoscopes, either the mobile or stationary hodoscope arrays ought to suffice at Fukushima, depending on

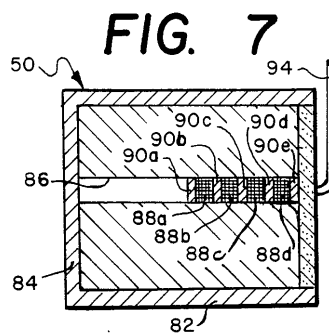
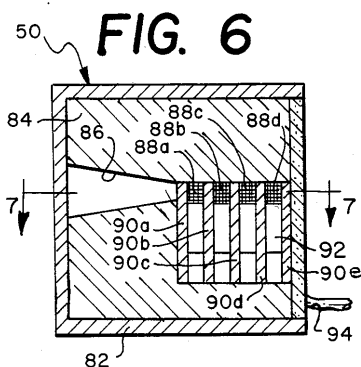
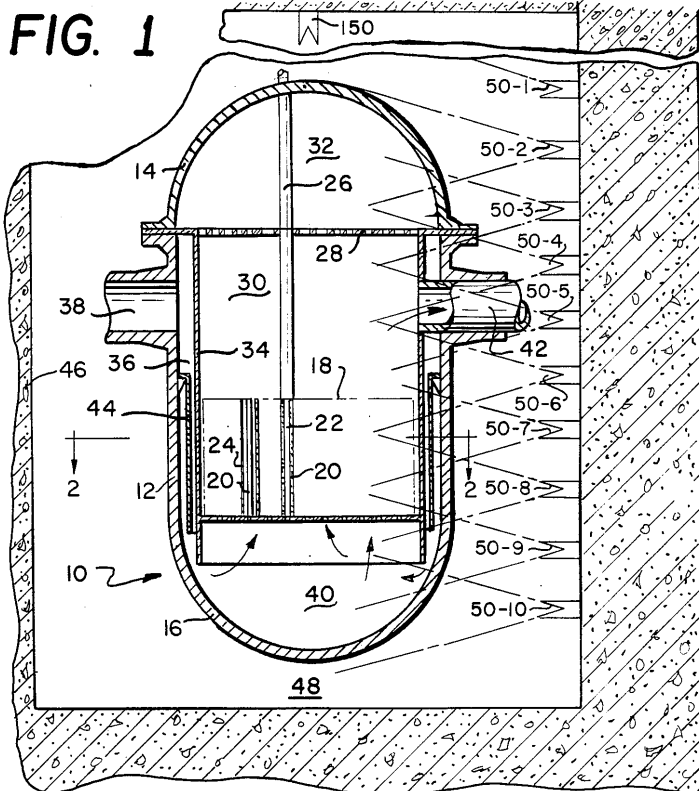
access that can be provided.

For the mobile system, a shielded and collimated hodoscope would have to be introduced through the airlock onto each Fukushima reactor floor at locations adjacent, but external to the reactor pressure vessels. The mobile system would be composed of a remotely linked pre-assembled array of collimated and calibrated radiation detectors, very similar to an arrangement operated at the TREAT reactor in the United States.

Figure 4.
Arrangement of Proposed Autonomous Hodoscope Detectors
Inside Containment of a Pressurized Water Reactor.

(Within the drawing, “Fig. 1” shows the elevational distribution of redundant detectors designated 50-1 through 50-10, while “Fig. 6” and “Fig. 7” show horizontal and vertical views of the shielded gamma-ray detectors.)

U.S. Patent Mar. 10, 1987 Sheet 1 of 5 4,649,015



The stationary version would be similar in some fundamental respects to that proposed in the TMI-inspired patent: It would consist of a vertical and radial array of detectors inserted in existing small-diameter penetrations through the biological shield, supplemented as necessary by additional drilled narrow holes.

Either system could be operated externally to produce remotely analyzed, reconstructed images of the residual internal core fuel, structural configuration, and coolant level. Validated data reconstructions could be shared as necessary with contractors, managers, government officials, and public stakeholders.

Either or both hodoscope systems, if assembled and operated on the basis of accumulated long-term experience, should provide information specific and essential for safe defueling and decommissioning of the damaged Fukushima reactors.

In addition, the stationary system could provide real-time guidance specific to the eventual removal of residual core and structural components, thus making the Fukushima decommissioning operation safer, while reducing the required dismantlement time.

Years ago, a Japanese nuclear agency (JAEA) supported a project in the United States to compile hodoscope data. As a matter of fact, much of the essential detectors and electronics at the TREAT reactor have been stored and preserved – presumably recoverable.

Foundation of Technical and Operational Experience

The U.S. Department of Energy and the Nuclear Regulatory Commission supported relevant programs of the 1960s through the 1990s to improve nuclear reactor safety. In research and development undertaken primarily at Argonne National Laboratory, very

successful external nuclear diagnostic instrumentation was developed to detect fuel, coolant, and structural materials inside a reactor.

This experience led to the two patents, the first being related to specific instrumentation used for real-time detection of such designated materials in a specialized test reactor. The second patent — as an aftermath of the TMI-2 accident — was an application to externally monitor coolant level and fuel disposition in an operating or shutdown water-cooled power reactor. Considerable experimental data and analytical analysis formed the foundation of the now-expired patents.

While the recommended instrumentation for water-cooled reactors was never implemented, hindsight implies it should have been. One major lesson to be derived from the TMI-2 accident is that independent devices are needed to measure and monitor such critical parameters as coolant water level in the reactor vessel. During the TMI-2 accident, the installed conventional instrumentation became operationally ineffective and functionally ambiguous.

For the disabled Fukushima reactor, such diagnostic instrumentation could still be of value. Three reactors remain in a tenuous condition with currently ill-defined distributions of fuel and coolant. These are circumstances that could yet lead to additional hazardous consequences and public alarm.

It is of inestimable value to have autonomous instrumentation that operates under separate physical principles and directly measure (nuclear) properties of importance. Information autonomy is especially important during emergency conditions, such as loss of electrical power.

The separate physical principle involved here uses nuclear detection, rather than indirect conventional information derived from pressure, flow, and temperature instrumentation. The properties of direct significance are the actual water level and fuel integrity.

During the emergencies at TMI and Fukushima, standard reactor instruments became inoperative; moreover, their signal output lacked crucial information value, and they were indirect rather than direct in relevancy.

Post-Accident Conditions at Fukushima

On 29 March 2012, the following informed message was posted on the Internet:

“One of Japan’s crippled nuclear reactors still has fatally high radiation levels and much less water to cool it than officials had estimated, according to an internal examination that renews doubts about the plant’s stability....

“Further analysis carried out by TEPCO [the reactor operator] on the state of the reactor cores after the earthquake on March 11th have revealed that the Unit 1 at Fukushima Daiichi was damaged much earlier than previously predicted.... [Moreover] molten fuel rods in reactors No 1, 2 and 3 have not only melted, but also breached their inner containment vessels and accumulated in the outer steel containment vessels. TEPCO did not acknowledge that even a partial meltdown could have occurred until [months after the accident]....

“The entire episode revealed how little the company actually understood of the conditions inside the plant’s reactors and the fragility of the cold shutdown.”

Because of the still-continuing tenuous circumstances cited above, Japanese government and reactor officials should be interested in utilizing the proposed autonomous hodoscope instrumentation in order to determine the still-uncertain coolant levels and the less-known condition of reactor fuel in the Fukushima reactors. While workers and management in Japan have done remarkable and disciplined work in preventing the loss of life, there is much that yet needs to be done for the safe, orderly, and timely decommissioning of the reactors. ■

Dr. Alexander DeVolpi’s research and development work in reactor safety grew in part from active military service in the U.S. Navy, followed by assignments as a Reservist at the Naval Research Laboratory in Washington, DC, and the Naval Radiological Defense Laboratory in San Francisco. This affiliation led to specific applications in reactor-safety research and instrumentation later developed and utilized at the Idaho Nuclear Engineering Laboratory. In later years, he moved on to applications involving arms control and treaty verification, which included technical assignments from the Defense Nuclear Agency and professional collaboration with many non-government organizations. He specialized in technology at Argonne National Laboratory, near Chicago, Illinois.

Laser Isotope Separation (LIS)

The Benefits of Laser Isotope Separation

MARK RAIZEN *



Our planet contains vast natural resources, still largely untapped. These resources hold the promise of detecting and treating cancer, saving energy, making new materials, and advancing basic science.

What are these valuable resources? Where can they be found? How can we make them available?

The answer to the first question is that the resources are *rare isotopes of the elements*. The answer to the second question is easy: these isotopes are literally in our midst, within the elements that make up our planet. The third question is the crux of the matter; isolating rare isotopes of elements has been extremely difficult because they have nearly the same physical and chemical properties as other, more common, isotopes of the same element. This is the reason that many rare isotopes are the most expensive commodity on earth, with a price that can be over one thousand times that of gold! This prohibitive cost severely limits the exploration of new applications and therapies.

Here are just two examples of rare isotopes that could be widely used if only they were less expensive: Nickel-64, a stable isotope with a natural abundance of only 1 percent. It can be converted in a medical accelerator to Copper-64 which is a short lived radio-isotope with great promise for PET scans and cancer therapy. Calcium-48 is a stable isotope with a natural abundance of 0.2 percent. It is used as a diagnostic for osteoporosis

in women, bone development in children, and for a basic physics experiment that may determine the mass of the neutrino.

The only method for separating such isotopes dates back more than eighty years. This method, known as the Calutron, relies on electron ionization of atoms, and separation by the charge-to-mass ratio. Although first used in the 1930s for separating uranium, they were replaced by the gas centrifuge which is limited mostly to that element. The Calutrons remained as general purpose, though inefficient, isotope separators. Today, these machines are only operating in Russia, with an obsolete technology that is facing imminent shut-down. Without an alternative approach, most rare isotopes will not be available in the future *at any price*. The looming shortage of crucial isotopes is a national priority, as indicated by a 2009 report of the Nuclear Science Advisory Committee to the Department of Energy, "Isotopes for the Nation's Future."

I recommend this report to anyone with an interest in the scope and uses of stable and radio-isotopes. One topic discussed in this report is laser isotope separation. Although isotopes are almost identical in every manner, the wavelengths of the atomic transitions of different isotopes are slightly shifted from one another.

This "isotope shift" makes it possible to excite only one isotope with a narrow-band laser, leaving the others unaffected. The common wisdom until now has been that one must use lasers to selectively ionize the desired atoms. However, it turns out that in order to have a large probability for ionization, very high laser power at multiple colors is required. The scale is so large that it required a government effort, with one dedicated goal: laser isotope separation of uranium. This effort was ultimately terminated in 1999, mainly due to the high cost and complexity of the lasers, and to the best of my knowledge is not being pursued. Laser separation of a molecular compound of uranium is still being pursued commercially by GE-Hitachi. I have followed this work

*Dr. Mark G. Raizen is the Sid W. Richardson Foundation Regents Chair and professor of physics at the University of Texas at Austin.

The Risks of Laser Isotope Separation

FRANCIS SLAKEY *

Over the last 15 years I've criss-crossed the globe and witnessed its full range of stories. And when you see dust kick up from the bare feet of a tribeswoman walking 5 miles to get water, you realize that we face enormous global challenges, including climate change, pandemics and access to clean water, to name just a few. Regardless of our individual views on any of those issues, I'm sure that we can all agree on one thing: let's not add more challenges to the list. We have enough to deal with.

So, when the research that we carry out has the possibility of creating significant risks, then we should pause, reflect, and make sure that we don't add yet another burden to an already challenged world.

Biologists did just that – pause and reflect – in exemplary fashion a few months ago when they confronted the H5N1 issue. Concerned about potential security risks associated with publishing particular work on airborne transmission of avian flu, the relevant community of biologists put a self-imposed pause on research to consider the implications and challenges. It was thoughtfully done, with only modest reluctance from some scientists, and with benefit to all.

We are now at a moment when it would be fruitful for the relevant members of the physics and engineering communities to carry out a similar examination of the risks and benefits of some areas of isotope separation research.

So far, we've gotten lucky in uncovering when countries are developing nuclear weapons programs. However, new isotope separation technologies are emerging that are smaller, more efficient and harder, if not impossible, to detect. The technologies are in various phases of development, from basic research to commercialization. Consider this:

- Global Laser Enrichment, a joint venture of General Electric-Hitachi, is constructing and evaluating a laser-based method of uranium enrichment (SILEX) that is substantially more efficient and could leave little prospect for detection if stolen and acquired by a rogue group.
- Professor Raizen has developed a method of single-photon isotope separation using a magnetic trap and low-power laser excitation for a



more efficient method to develop much-needed medical isotopes. His technique isn't intended to enrich uranium, although the potential may well be there.

These developments raise the same issue: the on-going push for greater efficiency in isotope separation carries associated proliferation risks.

These risks of more efficient isotope separation are well known to the U.S. government. For example, the SILEX technology under development in North Carolina was the subject of a multi-agency proliferation-assessment report. The report conceded that "Laser-based enrichment processes have always been of concern from the perspective of nuclear proliferation... a laser enrichment facility might be easier to build without detection and could be a more efficient producer of high enriched uranium for a nuclear weapons program."

The report ominously stated that it seemed likely that the technology would "renew interest in laser enrichment by nations with benign intent as well as by proliferants with an interest in finding an easier route to acquiring fissile material for nuclear weapons."

So the risks of enrichment technology are well documented, and the consequences of the proliferation of the technology are clear and present, most immediately in Iran.

** Dr. Francis Slakey is the Upjohn Lecturer on Physics and Public Policy and the co-Director of the Program on Science in the Public Interest at Georgetown University. He is also the Associate Director of Public Affairs for the American Physical Society.*

The Benefits of Laser Isotope Separation

MARK RAIZEN

from a distance, and always felt there must be a solution which would be simple and cost-effective for the many smaller-scale isotopes that are needed. It came from an unexpected direction.

Over the past few years, my research has focused on developing general methods for controlling the motion of atoms in gas phase. The successful realization of these methods uses single-photons to control the magnetic state of each atom, followed by magnetic manipulation. It has brought to reality a thought experiment by James Clerk Maxwell from 1870 known as

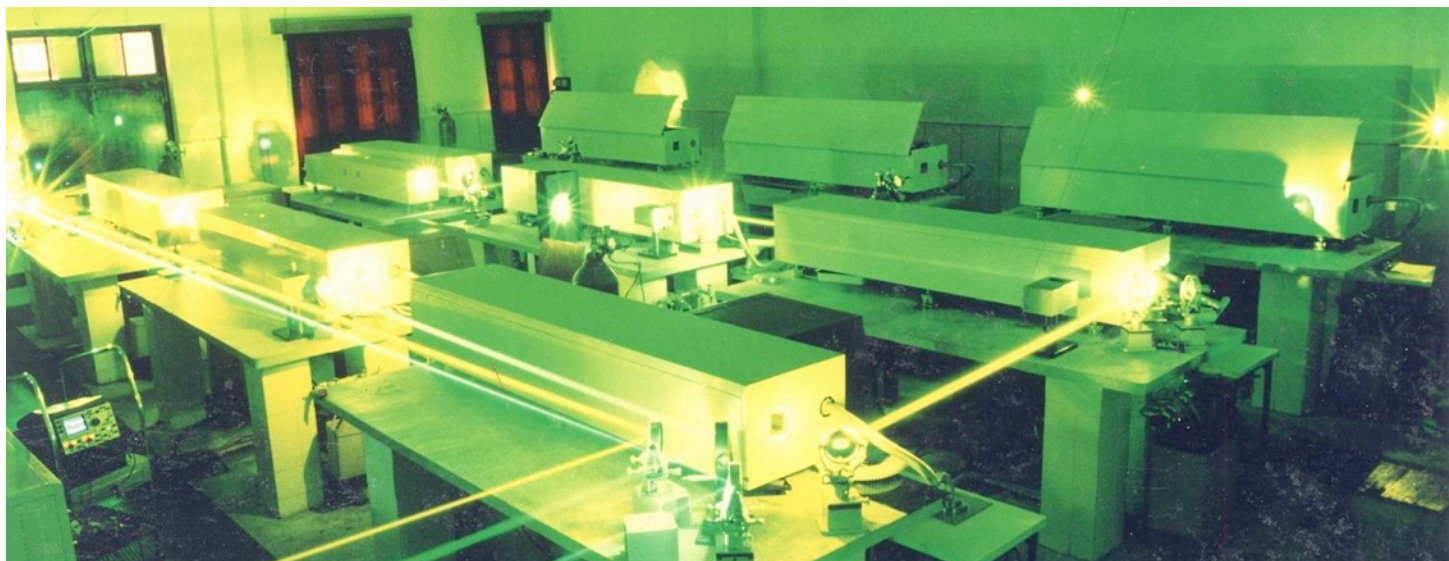
Maxwell's Demon. This work is reviewed in an article that I wrote for *Scientific American*, "Demons, Entropy, and the Quest for Absolute Zero," published in the March 2011 issue. I realized that these very same methods can also be used for efficient isotope separation with low-power solid-state lasers, a paradigm shift from ionization. We are pursuing this avenue with a proof-of-principle experiment, soon to be completed. This will then be applied commercially towards production of important medical isotopes, where the need is most urgent. In fact, this could save your life! ■

The Risks of Laser Isotope Separation

FRANCIS SLAKEY

Of course, the easiest path for our research community would be to claim that these risks are someone else's responsibility – we are scientists after all, not police. Yet, the biologists didn't take that easy path. They broadened their sense of responsibility outside of the lab. They paused, considered, deliberated. And there is a practical reason for doing this. If scientists don't consider the risks, we leave it to others to decide. And we may not like what they conclude.

What would we conclude from pausing and carrying out our own "stress test"? I can't predict the outcome. In the case of the biologists, they strengthened their system with a centerpiece called the National Science Advisory Board for Biosecurity that monitors "dual-use research of concern" and it has received enthusiastic endorsements from scientists. The biologists came out of the process stronger. So can we. ■



FAS MATTERS

FAS NEWS FROM DC HEADQUARTERS

2012 Nuclear Security Summit

In March 2012, the 2012 Nuclear Security Summit was held in Seoul, South Korea, where 53 heads of state and international organizations came together to discuss international cooperative measures to protect nuclear materials and facilities from terrorist groups. The Nuclear Security Summit has come at a critical juncture. Global terrorist attacks have prompted concerns about nuclear terrorism, and many states may continue to shop for nuclear reactors to meet their energy supply needs, despite the horrific incident at Japan's Fukushima Dai-ichi nuclear power plant. Against this backdrop, world leaders are charged with the difficult task of agreeing on measures that will secure vulnerable materials around the world. FAS recorded two podcasts featuring FAS President Dr. Charles D. Ferguson. In the first he examines the safety of U.S. nuclear power plants post-Fukushima. The second podcast focuses on the policies implemented as a result of the first nuclear summit held in Washington, DC 2010, and the significance of South Korea hosting the 2012 summit. Dr. Ferguson also discusses the security of radioactive materials, which was the subject of a new paper, "Ensuring the Security of Radioactive Sources," released in March 2012. Listen to the podcasts here: <http://www.fas.org/podcasts/>.

USA Science and Engineering Festival

On April 27 - 29, 2012, FAS staff worked a booth at the 2nd Annual USA Science and Engineering Festival in Washington, DC. FAS developed hands-on activities for kids interested in learning more about the role of science in policymaking. The goal of the festival is to reinvigorate the interest of our nation's youth in science, technology, engineering and math (STEM).

Non-Strategic Nuclear Weapons

On May 3, 2012, Hans Kristensen, director of the Nuclear Information Project, briefed congressional staffers on Capitol Hill on a new FAS Special Report on "Non-Strategic Nuclear Weapons" published three weeks before 28 NATO member countries convened in Chicago in May 2012 to approve the conclusions of a year-long Deterrence and Defense Posture Review (DDPR). Among other issues, the review determined the role of the U.S. non-strategic nuclear weapons deployed in Europe and how NATO might work to reduce its nuclear posture as well as Russia's inventory of such weapons in the future. Lack of transparency fuels mistrust and worst-case assumptions, and the concerns some eastern NATO countries have about Russia have been used to prevent a withdrawal of the remaining U.S. nuclear weapons from Europe. The report concludes that non-strategic nuclear weapons are neither the reason nor the solution for Europe's security issues today but that lack of political leadership has allowed bureaucrats to give these weapons a legitimacy they don't possess and shouldn't have. Read the report here: <http://www.fas.org/pubs/reports/nsnw.html>.

FAS MATTERS

FAS NEWS FROM DC HEADQUARTERS

Bridging the Generational Divide in Nuclear Security

On May 8, 2012, FAS hosted an event on how to bridge the generational divide on nuclear security. FAS works to engage young scientists and engineers in important security issues. FAS President Dr. Charles D. Ferguson revealed the many ways in which FAS is reaching out to the next generation, like the new Nuclear Transparency Project and the Security Scholars Program. FAS also recognized the Honorable Rose Gottemoeller, Acting Under Secretary for Arms Control and International Security, as well as Assistant Secretary for Arms Control, Verification and Compliance, and Dr. Sidney Drell, Deputy Director Emeritus of the SLAC National Accelerator Laboratory at Stanford University, for their work towards a nuclear free world at the Reykjavik Awards Ceremony and luncheon at the Menlo Circus Club in Atherton, California. The Master of Ceremonies was Dr. Ferguson. Learn more here: <http://www.fas.org/press/events/reykjavik.html>.

FAS Security Scholars

Launched as part of FAS's new Science and Security Initiative, the Security Scholars Program provides students with experience in science and security policy. FAS staff and members from government, academia and policy fields mentor scholars on collaborative and independent research. Through this partnership, scholars contribute to the ongoing security debate with reports, articles and blog posts for publications and FAS.org website. This summer, FAS hosted four scholars who conducted research on cyber security, Brazil's uses of nuclear technology, Pakistan's nuclear weapons, and security challenges related to climate change. To learn more, please visit: <http://www.fas.org/about/security-scholars.html>

FALL ISSUE OF PIR

- Pakistan's Nuclear Weapons
- Brazil's Nuclear Future
- The Homegrown Threat
- Continuing Terrorist Threats
- How Prepared Are First Responders?

The PIR welcomes letters to the editor. Letters should not exceed 300 words and may be edited for length and clarity. The deadline for the Fall issue is **September 21, 2012**. To submit a letter, please email pir@fas.org or fax 202-675-1010.

To learn about advertising opportunities in print and online please call (202) 454-4680 or email advertising@fas.org.

THE FAS AWARDS DINNER AND CEREMONY

On February 6, 2012, FAS held the 2011 Awards Ceremony at the Carnegie Institution for Science in Washington, DC.

The Honorable Steven Chu, the United States Secretary of Energy, received the 2011 Hans Bethe Award.

The inaugural 2011 Richard L. Garwin Award was presented to **Dr. Richard A. Meserve**, President of the Carnegie Institution of Science.

The evening's Master of Ceremonies was **Dr. John Holdren**, the Director of the White House Office of Science and Technology Policy and Science Advisor to the President of the United States.

For more information, to watch video, see images and view the powerpoint, please visit:
www.FAS.org/about/2011awards.html.

FAS THANKS THE 2011 SPONSORS

GOLD

**General Atomics
HBO**

SILVER

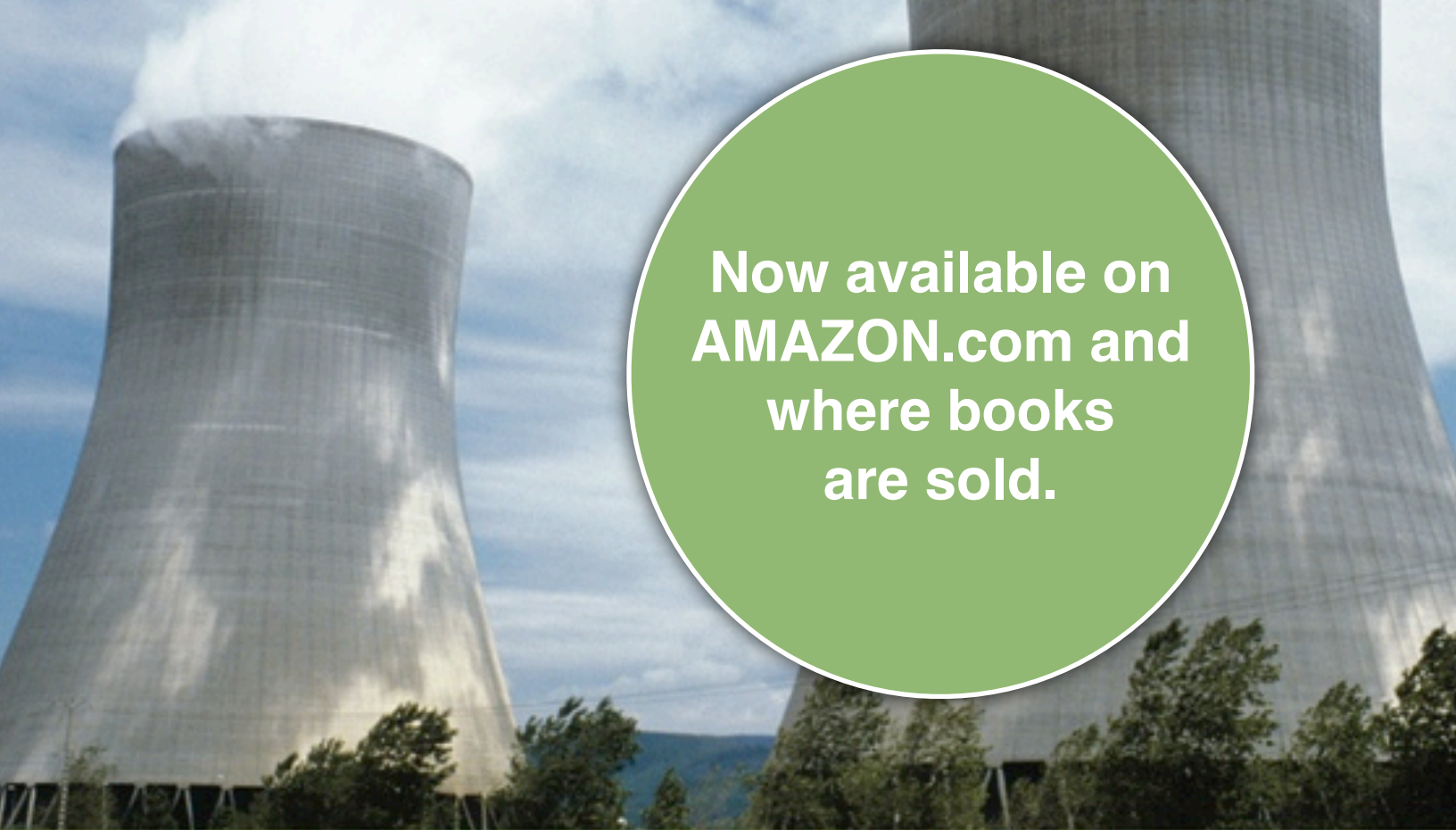
**BP America
Denjiren/The Federation of Electric
Power Companies of Japan
Lawrence Brown**

BRONZE

**Babcock & Wilcox
GABI
Energy Future Holdings/TXU
Fairview Builders, LLC**

**Wine was compliments of
Fairview Builders, LLC.**



A photograph of two large, grey, hyperboloid cooling towers of a nuclear power plant. The towers are set against a blue sky with scattered white clouds. In the foreground, there are green trees and some industrial structures. A large green circle with a white border is overlaid on the right side of the image.

Now available on
AMAZON.com and
where books
are sold.

NUCLEAR ENERGY

WHAT EVERYONE NEEDS TO KNOW

CHARLES D. FERGUSON