RAND REVIEW

Summer 2014

Vol. 38, No. 2

WILD WILD WEB

For Now, Cybercrime Has the Upper Hand in Its Duel with the Law

By Lillian Ablon and Martin C. Libicki

RAND CORPORATION

ALSO IN THIS ISSUE

Medical Innovation • Security Cooperation • Victor Hugo Evocation

Innovative Devices, Same Old Vices

TWO OF THE LEAD STORIES IN THIS ISSUE serve as humbling reminders that even the most dazzling and ingenious technological advancements often function as mere conduits for the basest instincts of apish humans who get their grubby hands all over them.

The Internet and social media have made people everywhere more productive and interconnected—including resourceful and entrepreneurial criminals everywhere who are eager to interconnect with your credit card numbers and Twitter accounts. Meanwhile, modern medical innovations might be the most wonderfully beneficial inventions that many of us will ever have the great fortune to experience; but the great fortune arising from these inventions is sometimes calculated to accrue not in the form of improved health but rather in the form of maximized profits at taxpayer expense.

Like the lawman of old pacing toward the cyber horizon on our cover, government officials and private-sector leaders today need to guide those who inhabit our social and medical frontiers toward decent practices that do justice to the citizenry's own ingenuity. Our cover story explains how law enforcement and other government agencies, along with commercial companies, could rise to the challenge to fight cybercrime, while our spread on medical innovation outlines how policymakers should replace the casino-like U.S. market for new medical technologies with something geared toward nobler ends.

One of those nobler ends is exemplified by the surgically implantable chip that Arati Prabhakar, director of the Defense Advanced Research Projects Agency, described during her presentation at the RAND Corporation in May. The breathtaking medical frontier that she discusses briefly in the "Common Ground" section of this magazine can revive your faith in the most exalted capacities of even those apish humans.

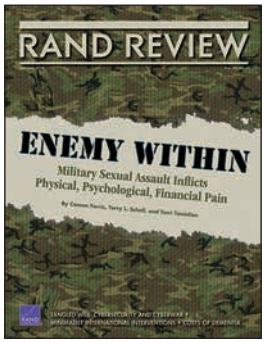
—John Godges

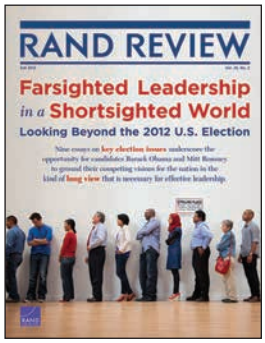
Cover credits
LAWMAN: ©ISTOCK.COM/NELSONARTS; CYBER SKY: ©ISTOCK.COM/NADDI; DESIGN: EILEEN DELSON LA RUSSO

The Internet and social media have made people everywhere more productive and interconnected—including resourceful and entrepreneurial criminals everywhere who are eager to interconnect with your credit card numbers and Twitter accounts.

Get the Big Picture

RAND Review covers the big issues
with an eye for the important details.





For previous editions and free online subscriptions, visit www.randreview.org

RAND REVIEW

The Flagship Magazine of the RAND Corporation

Summer 2014 ▪ Vol. 38, No. 2

Editor-in-Chief
John Godges

Associate Editor
Scott Orr

Assistant Editor
James Torr

Proofreader
Kelly Schwartz

Designer
Eileen Delson La Russo

Graphic Artist
Sandra Petitjean

Photographer
Diane Baldwin

Production Editor
Todd Duft

Circulation Coordinator
Nora Kerrigan

Web Producers
Lee Floyd, Joel Kline, April Stock, Jason Walkowiak, Chara Williams

Editorial Board
Winfield Boerckel, Timothy Bonds, Brent Bradley, Cynthia Cook, Jennifer Gould, Jeffrey Hiday, James Hosek, Iao Katagiri, Carl Rhodes, K. Jack Riley, Charlene Rohr, Brian Stecher, Terri Tanielian, Mary Vaiana

RAND Board of Trustees
Karen Elliott House (chair), Richard J. Danzig (vice chair), Sheila Bair, Barbara Barrett, Kenneth R. Feinberg, Francis Fukuyama, Pedro José Greer, Jr., Bonnie Hill, Ann McLaughlin Korologos, Philip Lader, Michael E. Leiter, Peter Lowy, James M. Loy, Michael Lynton, Ronald L. Olson, Mary E. Peters, Donald B. Rice, Michael D. Rich, David K. Richards, Hector Ruiz, Leonard D. Schaeffer

Trustees Emeriti
Harold Brown, Frank C. Carlucci

RAND Review is published periodically by the RAND Corporation, a nonprofit organization. The mission of the RAND Corporation is to help improve policy and decisionmaking through research and analysis. Opinions are those of the authors and do not reflect positions taken by RAND, its board, or its clients.

LETTERS Send letters to: Editor, *RAND Review*, 1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138, or e-mail letters@rand.org

PERMISSIONS For information about using material published in *RAND Review*, visit www.rand.org/publications/permissions/

COPIES For hard copies of *RAND Review*, call (877) 584-8642 (toll free) or (310) 451-7002 (outside the United States); send a fax to (412) 802-4981; or e-mail order@rand.org

REPORTS Most reports cited in these pages may be purchased. To place credit card orders, contact RAND at the phone numbers or e-mail address listed immediately above. National Book Network (NBN) also carries selected RAND titles. Call NBN at (800) 462-6420.

SEARCH RAND documents can be searched by author, title, and category at www.rand.org/search/pubs_search/

© Copyright 2014 RAND Corporation
RAND is a registered trademark.

RAND: OBJECTIVE ANALYSIS. EFFECTIVE SOLUTIONS.

www.rand.org

Contents

COVER STORY

WILD WILD WEB
For now, cybercrime has the upper hand in its duel with the law
Lillian Ablon and Martin C. Libicki 12

FEATURES

Cut the Crapshoot 10
For medical innovation worth the gamble, it's time to close the casino

From Azerbaijan to Zambia 20
Security cooperation bears fruit, depending on the type of soil and the type of seeds

DEPARTMENTS

4 PUBLIC SQUARE—A MEETING PLACE FOR RAND VOICES

- Telehealth
- Homeland security
- Long-term care for dementia
- Prisoner exchanges
- Disproven Western assumptions
- Frankensteins in Ukraine
- Imposing peace in Syria
- Investing in Africa
- Putin's weakness
- NATO's strength

8 NUMBERS IN THE NEWS

A TRIA Tipping Point
If the U.S. Congress allows the Terrorism Risk Insurance Act to expire, federal spending would grow for terrorism losses below $50 billion

9 COMMON GROUND—A FORUM FOR RAND GUEST SPEAKERS

Barrier-Breaking Stories ▪ Breathtaking Medical Frontiers

22 PUBLISHER'S PAGE

The Telescope and the Microscope
Public policy wisdom from Victor Hugo
Michael D. Rich

Government Testimonies

On Telehealth

"Telehealth and other innovations can be cheaper than an in-person visit on a per-visit basis. However, lower cost per visit does not ensure telehealth will reduce costs. The concern is that telehealth could increase costs by driving greater utilization of health care services. In other words, people who otherwise would not have sought care in the first place will use telehealth to get care. If this increased access and greater utilization leads to treatment that leads to improved health, then this new utilization is good for our society. If, however, this new use is overutilization, care that does not lead to improvements in health, then there could be increased costs without any added health benefits. The very advantage of telehealth, its ability to make care convenient, is also potentially its Achilles' heel. The growth of telehealth requires oversight to ensure that these new delivery models do three things: provide high-quality care, improve access to those who need it most, and [be] utilized in a cost-effective manner."

Ateev Mehrotra, *policy analyst, in testimony presented before the U.S. House Energy and Commerce Committee, Subcommittee on Health, May 1, 2014*

"Lower cost per visit does not ensure telehealth will reduce costs."

On Homeland Security

"Fear of terrorism matters. Numerous studies demonstrate that even if other hazards threaten the same number of lives or economic activity, people are more concerned about terrorism events than other events, support spending more for terrorism security, and are willing to cede more liberties in the name of terrorism security. However, in reality, all terrorist events do not pose the same risks as other hazards. There are many disasters, accidents, and crimes that have historically threatened more lives, caused more economic damage, and led to more societal disruption than terrorism. We all certainly want more effective protection from terrorism, better preparation for disasters, and more resilient communities. Three things will be required: *strategic focus* to direct resources where they are most needed, *strong oversight* to assure that resources are used effectively, and finally, *cooperation across government* to improve efficiency."

Henry H. Willis, *director of RAND's Homeland Security and Defense Center, in testimony presented before the U.S. House Homeland Security Committee, Subcommittee on Oversight and Management Efficiency, June 20, 2014*

"People are more concerned about terrorism events than other events."

On Care for Dementia

"Most households will not incur large costs for dementia care: Many patients will have their care covered by Medicaid or private long-term care insurance. Their nursing-home or hospitalization stays may be short and relatively affordable. However, other households may face great costs because of nursing-home stays of five years or more. Thus, a minority of families may face financially devastating costs. This situation, in which many families incur minor costs but a few incur very large costs, ought to call for an insurance solution, one in which the costs of long-term care could be spread across the entire population rather than being concentrated on the unlucky few. At the moment, the long-term-care insurance products that are available apparently do not meet the needs of the older population, as evidenced by the very low take-up rates, about 13 percent in the population age 55 or older. Better designed products to reduce the risk of very large out-of-pocket spending for long-term care would help reduce a significant cause of concern for the older population."

Michael D. Hurd, *director of the RAND Center for the Study of Aging, in testimony presented before the U.S. Senate Appropriations Committee, Subcommittee on Labor, Health and Human Services, Education, and Related Agencies, on February 26, 2014*

"This situation ought to call for an insurance solution."

OVER THE AIRWAVES

A History of Prisoner Exchanges

"We have exchanged prisoners with Nazi Germany. We've exchanged prisoners with communist North Korea. We've exchanged prisoners every time we've fought a war, and we don't exchange just the good guys. We exchange whoever's there. As for, 'Are these guys the worst of the worst?' Well, there are a lot of pretty bad guys out there. And a lot of people just as bad as these are people we've done deals with."

Jonah Blank, political scientist, upon the release of U.S. Army Sgt. Bowe Bergdahl in exchange for five Taliban prisoners held at Guantánamo Bay, on *Slate.com*, June 3, 2014

Listen to the Slate interview

> "We've exchanged prisoners every time we've fought a war."

Ukraine: Two Disproven Assumptions

"U.S. and Western policy was based on two fundamental assumptions. One was that Europe was stable and secure and that the U.S. could begin to focus on other areas, particularly Asia and the Middle East—and [the other was] that Russia was more a partner than an adversary. The actions in Crimea have undermined and challenged both of those assumptions about U.S. and Western foreign policy. Therefore, there needs to be a strong and vital response. NATO has to do more to reassure the Baltics, Poland, and Romania, and this cannot be a unilateral U.S. reinforcement. It has to be a NATO reinforcement. The U.S. can provide the bulk of the troops, but it's very important that other NATO members also contribute."

F. Stephen Larrabee, distinguished chair in European security, on *BBC World News*, June 4, 2014

> "NATO has to do more to reassure the Baltics, Poland, and Romania."

Ukraine: Forces of Frankensteins

"My own view is that the Kremlin has encouraged these separatists but that they've created something of a Frankenstein monster, which now it's not certain that they really control. One of the things we want to be watching is whether or not the Kremlin really does try to cooperate with [Ukrainian President Petro] Poroshenko in reining them in, or at least tacitly accepts his efforts to do so."

Christopher Chivvis, political scientist, on *Bloomberg Television*, May 27, 2014

Watch the Bloomberg segment

RADIO ANTENNA: IMAGE VIA VANFAN/FOTOLIA;
FLAGS: IMAGE VIA LEONARD ZHUKOVSKY/FOTOLIA

Proposal for Syria and Iraq: An Imposed Peace

"THE RECENT JIHADIST SEIZURE of two major cities in northern Iraq, Mosul and Tikrit, is a clear indicator that the spillover of violence from the Syrian civil war is rapidly reshaping the Middle East. What to do? The answer may lie in a negotiated settlement, which includes negotiating with Syrian President Bashar Assad, perhaps brokered through the Russians and Iranians. A settlement with the regime in Damascus, in the form of an imposed peace over selected safe zones within Syria that would protect segments of the Syrian population most likely to suffer at the hands of Assad's forces and guarded by an international stabilization force, would enable Assad to reconsolidate areas of the country under his control and reverse—or at least slow—the destabilization of the region. Assad has much to gain from this proposal, as do Tehran and Baghdad. In turn, Assad could help NATO and other willing partners focus time and resources on ISIS [the Islamic State of Iraq and Syria], which poses the greatest threat to the Middle East, the United States, and Europe."

William Young, policy analyst, in *USA Today*, June 14, 2014

"A settlement with the regime in Damascus would reverse—or at least slow—the destabilization of the region."

Investments in Africa

"Secretary of State John Kerry and Chinese Premier Li Keqiang both made high-profile visits to Africa within a week of each other this month. Kerry sought to resolve the continuing violence in South Sudan and the Central African Republic, Li came bearing aid and investment deals. The United States could learn something from Beijing's economic playbook. As Washington seeks to defuse conflict and reduce security threats across the continent, it should do far more to promote trade and investment in ways that benefit both U.S. business and African economies. By supporting Africa's economic and commercial development, greater U.S. business engagement can also strengthen security and stability throughout the region."

Larry Hanauer, international policy analyst, and **Lyle Morris**, project associate, on Reuters.com, May 30, 2014

"The United States could learn something from Beijing's economic playbook."

Chinese Premier Li Keqiang announces a new railway agreement at the State House in Nairobi, Kenya, on May 11, 2014. Flanking him are Uganda's President Yoweri Museveni, Kenya's President Uhuru Kenyatta, Rwanda's President Paul Kagame, and South Sudan's President Salva Kiir.

REUTERS/THOMAS MUKOYA

Putin's Weakness

"[Russian President Vladimir] Putin shows all the signs of following in the footsteps of history's most infamous blunderers, and the decision-making traits he exhibits are both familiar and ominous. Leaders who make big strategic mistakes are often afflicted with excessive hubris. Both Napoleon in 1812 and Hitler in 1941 had gained a string of decisive battlefield victories, which gave them a sense of invincibility, if not destiny. Both, of course, invaded Russia and lost massive armies. Putin's hubris is not based upon a string of military victories, however, but upon a conviction that he knows how to intimidate Russia's neighbors. He has occupied two provinces of Georgia, directed cyberwarfare against Estonia, threatened Poland with nuclear missiles, manipulated the dependence of customers on Russian gas, and sought to provoke unrest among Russian minorities in other countries. He appears to think that the seizure of Crimea is a great success—ignoring the self-harm it will do—which reinforces his belief that he is in control, and that he can write a script in which others will meekly play their assigned roles. Such unwarranted confidence is a classic cognitive flaw that correlates strongly with a potential to commit blunders."

David C. Gompert, formerly principal deputy director for national intelligence, and **Hans Binnendijk**, formerly director of the Institute for National Strategic Studies, and both senior RAND fellows, in *Foreign Policy*, April 14, 2014

"Leaders who make big strategic mistakes are often afflicted with excessive hubris."

NATO's Strength

"Despite the smaller number of U.S. troops in Europe, the military balance there is far more favorable to NATO today than it was when nearly 10 times as many American soldiers, sailors, and airmen were stationed on the continent. The reason for this is simple and obvious: the disastrous—from Moscow's point of view—revision of the overall European security environment that began in the early 1990s. Yes, the United States has many fewer forces in Europe than it did in 1989. But Russia has none, its allies have all switched sides, and its military is but a shadow of what it was 25 years ago. When he examines the European balance of power, Russian President Vladimir Putin undoubtedly sees that the Russian army is outgunned. This should help deter him from further aggression in the region; whether or not it will is another question."

David Shlapak, international policy analyst, in *U.S. News & World Report*, April 9, 2014

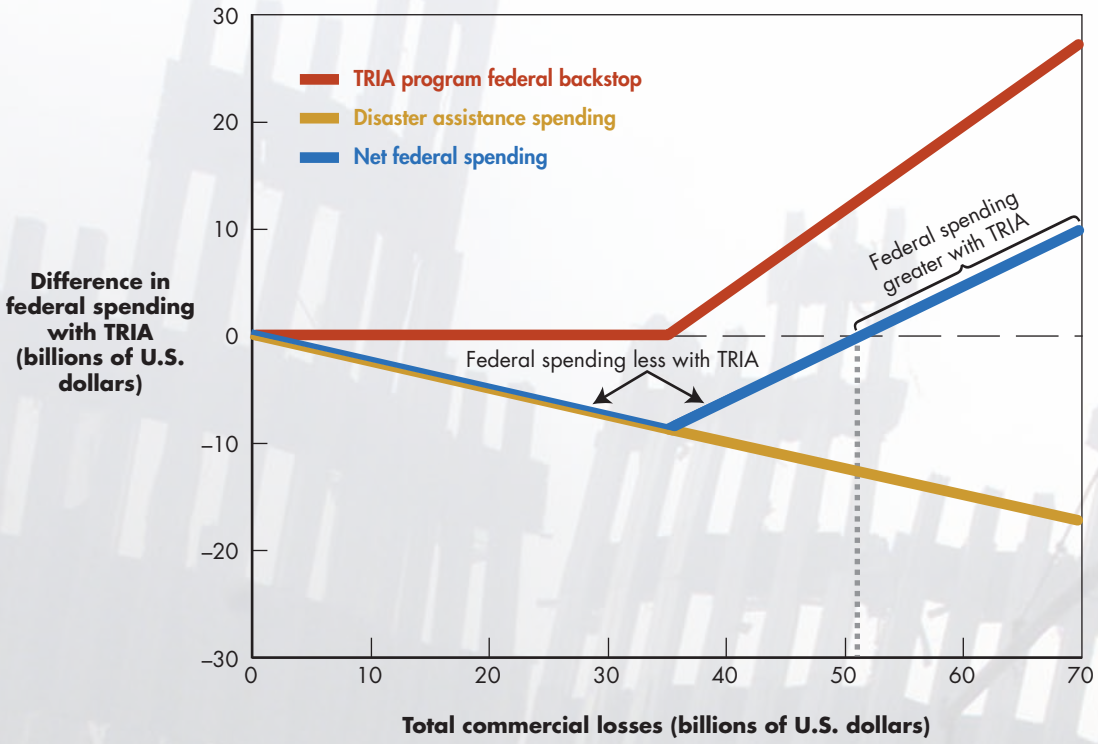
"Yes, the United States has many fewer forces in Europe than it did in 1989. But Russia has none."

Above: A towering papier-mâché caricature of Russian President Vladimir Putin, with his bicep depicted as a "Crimea" bomb, rode on a parade float high above the crowds in the traditional Rose Monday parade in Düsseldorf, Germany, on March 3, 2014.

REUTERS/INA FASSBENDER

A TRIA Tipping Point

If the U.S. Congress Allows the Terrorism Risk Insurance Act to Expire, Federal Spending Would Grow for Terrorism Losses Below $50 Billion



ENACTED IN NOVEMBER 2002 and extended first in 2005 and again in 2007, the U.S. Terrorism Risk Insurance Act (TRIA) will expire in December 2014 unless Congress extends it once again. RAND researchers found that TRIA is expected to save taxpayers money in the event of a terrorist attack comparable to any experienced before.

TRIA influences federal spending in two ways. The first is through a federal "backstop" on catastrophic terrorism losses (the red curve in the figure). Under TRIA, the insurance industry and commercial policyholders must pay all eligible insured terrorism losses up to at least $27.5 billion annually. (At current coverage rates for terrorism, insured losses of $27.5 billion would correspond to total commercial losses of about $35 billion.) For attacks with greater losses, the federal government pays a portion of the insured losses.

The second way that TRIA affects federal spending is by making a functioning terrorism insurance market possible. According to insurance industry projections, allowing TRIA to expire would reduce the amount of terrorism insurance coverage purchased, leading to twice the uninsured losses and hence twice the demand for federal disaster assistance. (The gold curve in the figure represents the reduced disaster assistance spending under TRIA.)

For attacks that result in more than $35 billion in total commercial losses, federal spending on catastrophic losses would kick in, but federal spending on disaster assistance would continue to fall because of TRIA. (The blue curve in the figure represents the best estimate of the net effect.)

For annual terrorist attack losses up to about $50 billion, federal spending would be less with TRIA than without it. For losses of more than about $50 billion, the TRIA backstop would dominate, and the federal government would pay more with TRIA than without it.

The 9/11 terrorist attacks inflicted total commercial losses of about $40 billion (in current dollars). Thus, for attacks on the scale of anything experienced before, TRIA is likely to save taxpayers billions of dollars.

SOURCE: *The Impact on Federal Spending of Allowing the Terrorism Risk Insurance Act to Expire*, Tom LaTourrette, Noreen Clancy, RAND/RR-611-CCRMC, 2014, 19 pp., www.rand.org/t/RR611

REUTERS/PETER MORGAN

PHOTO BY DIANE BALDWIN

Watch highlights from the speech

Barrier-Breaking Stories

"Storytelling is an ancient and underappreciated element of public life. Think of Christ's parables in the Bible or Plato's dialogues—both used stories to communicate, inform, persuade, and inspire action. In the American experience, think of Harriet Beecher Stowe's *Uncle Tom's Cabin*, which fueled the abolitionist movement prior to the Civil War, or Upton Sinclair's *The Jungle*, which contributed to a wave of reform and regulation in American industry. However they are communicated—by word of mouth, speeches, books, films, or the Internet—stories have the ability to touch listeners in a way that the cold hard facts, on their own, never can. In truth, our ability to tell a story effectively enables us to break through barriers, overcome resistance, change minds, and even change the world."

—**Former Senator Elizabeth Dole,** speaking at the Commencement Exercises of the Pardee RAND Graduate School, June 21, 2014

Breathtaking Medical Frontiers

"One of our patients is a woman named Jan. Jan has been a quadriplegic for a number of years. A chip has been surgically emplaced on her neocortex. It's a small probe. What it does is it picks up the electrical signals from the region of her brain that we knew was going to be associated with some motor-control signaling. Those electrical signals come out to these ports that are on her head. Those signals are then being used to control this prosthetic arm. When I realized that Jan was not controlling one finger or one muscle at a time but really it was this kind of near natural control, that's when I realized that we had opened a door. In a sense, we have freed the brain from the body, and the opportunities that lie ahead could go in almost any conceivable direction."

—**Arati Prabhakar,** director of the Defense Advanced Research Projects Agency, delivering the Haskins Lecture on Science Policy at the RAND Corporation, May 8, 2014

PHOTO BY ALEX COHEN

Listen to the podcast

CUT THE CRAPSHOOT

For Medical Innovation Worth the Gamble, It's Time to Close the Casino

U.S. POLICYMAKERS NEED TO COUNTERACT THE PERVERSE FINANCIAL INCENTIVES that induce inventors and investors to bet big on new medical technologies that offer the highest payouts without substantially improving health. Costly new technology is a primary driver of health care spending. This should come as no surprise, because all players in the dicey U.S. market for new medical technologies—inventors, investors, payers, providers, and patients—face long odds if they want to put money on products that could curb health spending while also boosting health. The rules of the game need to change.

Here are ten ways to fix the defective incentive system

Five ways to reduce the costs
and risks of invention and approval

Enable More Creativity in Funding Basic Science

When the U.S. National Institutes of Health (NIH) selects research to fund, it typically favors low-risk projects. If investigators fail to achieve their project goals, prospects for future NIH funding are greatly reduced. The Howard Hughes Medical Institute employs a different model: It funds scientists rather than projects, encourages risk-taking, and seems more willing than NIH to keep funding the promising scientists whose past risky endeavors did not pan out.

Offer Prizes for Inventions

Substantial prizes could be awarded to the first individual or group that invents a drug or device that satisfies pre-specified criteria. Prizes could be offered by such public entities as NIH or the Centers for Medicare and Medicaid Services (CMS), private health care systems, philanthropists, charitable foundations, and public-private partnerships. An alternative to an immediate cash prize is to offer winners a percentage of future Medicare savings attributed to the inventions. Federal legislation would be required to enable CMS to offer prizes.

Buy Out Patents

Purchasing patents of products already invented and likely to reduce spending could commercialize them at lower prices while immediately rewarding inventors. Public agencies, philanthropists, or public-private partnerships that purchase such patents could put them in the public domain to generate price competition or could license the technology, stipulating the highest price a licensee could charge. Again, the best approach might be to offer patent sellers a share of Medicare savings attributed to the inventions.

Establish a Public-Interest Investment Fund

Private investors often find the likely market rewards for inventing products that reduce spending too low to be attractive. But a public-interest investment fund could provide the required investment capital. A public-private partnership such as this could also tap the expertise of private-sector investors who are most capable of assessing the promise of technical concepts and inventors. As motivation, investors could be allowed to invest in projects supported by the fund, and the payoffs could once again include shared Medicare savings.

Expedite FDA Reviews and Approvals for Some Products

The U.S. Food and Drug Administration (FDA) could offer expedited—but not watered-down—review and approval processes for medical products with clear potential to substantially reduce health care spending. Expediting these processes could lower the regulatory costs and risks for inventors involved in gaining FDA approval. This change would require new legislation to expand the FDA's mission beyond ensuring safety and efficacy to include reducing health expenditures.

Five ways to shift profits
toward higher-value, lower-cost products

Reform Medicare Payment Policies

If new legislation were to allow CMS to consider cost in determining Medicare payment rates, the agency could set rates to save money and to raise profits on cost-saving inventions. One possibility is for Medicare to move away from fee-for-service payments to adopt approaches—such as bundled and capitated payment arrangements—that put providers at risk for costs not needed to deliver high-quality care. This would tend to boost demand for new cost-saving drugs, devices, and other health care technologies.

Reform Medicare Coverage Policies

Medicare could stop paying for tests, procedures, and products deemed by clinical experts to be ineffective or inappropriate. Medicare could also stop covering "off-label" (unapproved) uses of some very expensive cancer and other specialty drugs in circumstances for which there is little or no evidence of effectiveness. Expanding the use of palliative and hospice care in lieu of such drugs for terminally ill patients could also reduce spending. Some of these changes would require new legislation.

Coordinate FDA Approval and CMS Coverage Processes

For those products likely to help reduce spending, the CMS processes for determining Medicare coverage and payments could be coordinated with the FDA review and approval processes for ensuring safety and efficacy. This coordination could reduce the time required to move a product to market, thus cutting the costs and delays for manufacturers. Lessons learned from current efforts involving parallel review by FDA and CMS could help identify the best approach.

Increase Demand for Products That Decrease Spending

Higher demand for high-value products and lower demand for low-value products will require realigning incentives for providers and patients. One promising possibility is to expand the use of value-based insurance designs (VBIDs), which require patients to pay more out of pocket for services that are less likely to benefit them. A major challenge in implementing VBIDs is determining which services are more and less likely to substantially benefit individual patients. Therefore, it will also be necessary to . . .

. . . Increase Timely Technology Assessments

Health technology assessments (HTAs) provide evidence about the safety, efficacy, and cost of drugs, devices, and procedures—and in what circumstances it is appropriate to use them. Because medical technology evolves quickly, HTAs are more useful when they are more current. One emerging commercial model could offer a good way to produce more-timely HTAs: keeping abreast of the literature through fairly frequent searches and revising the HTAs when new findings warrant.

SOURCE: *Redirecting Innovation in U.S. Health Care: Options to Decrease Spending and Increase Value*, Steven Garber, Susan M. Gates, Emmett B. Keeler, Mary E. Vaiana, Andrew W. Mulcahy, Christopher Lau, Arthur L. Kellermann, RR-308, 2014, 130 pp., www.rand.org/t/RR308

PHOTO, FACING PAGE: IMAGE VIA RACHWAL/FOTOLIA; CADUCEUS: IMAGE VIA KRODESIGNS/FOTOLIA; DICE: IMAGES VIA DENIS FONCHIKO/FOTOLIA; DESIGN: DORI GORDON WALKER

WILD WI

For Now, Cybercrime Has the Upp

From shady trading posts to rough-and-ready roundups, from wanted posters to "bug bounties," the World Wide Web (and thus the whole world) has become vast untamed territory for those bent on cybercrime. But will there be a proverbial new sheriff in town? Only if law enforcement agencies rise to the challenge and if private companies harness the power of their legitimate markets to quell the illegitimate ones.

ILD WEB

per Hand in Its Duel with the Law

BY LILLIAN ABLON AND MARTIN C. LIBICKI

Black markets for computer-hacking tools, services, and by-products, including stolen credit card numbers, continue to grow, posing threats to businesses, governments, and individuals. The most prominent recent example was the capture of an estimated 40 million credit card numbers and 70 million user accounts in the December 2013 breach of retail giant Target. Within days, those data appeared—available for purchase—on black market websites.

The markets for cybercrime products and by-products have become so pervasive and accessible that the malicious hacking trade today can be, in certain respects and for some, more lucrative and easier to carry out than the illegal drug trade. Once the domain of lone hackers, cybercrime has become a burgeoning powerhouse of highly organized groups, often tied to drug cartels, mafias, terrorist cells, and even nation-states. It has matured into specialized markets, in which those who have gained the greatest access deal freely in the tools and spoils of the trade: exploit kits (software for creating, distributing, and managing attacks), botnets (remotely controlled computers used for sending spam or flooding websites), "as-a-service" offerings (hacking for hire), compromised hosts, and a continually flooded market for stolen credit card numbers and other personal credentials.

Consumers and businesses have fortified their data systems in response, but hackers have come back stronger. Increased arrests, meanwhile, spur increased media attention, which advertises the lucrative markets to those once unaware of the possibilities and reveals the tactics and techniques of law enforcement to those already in the markets, causing them to adapt. As more participants enter the market, and as current participants upgrade their methods of conducting business, the increasingly competitive and resilient hackers go after bigger targets and become harder to take down.

Everything from insulin pumps and pacemakers to cars, toasters, and refrigerators will offer malicious hackers networked points of entry.

As a result, the ability to attack is outpacing the ability to defend. Hyper-connectivity—particularly through the rise of the "Internet of Things"—will create even more opportunities for attack, as everything from insulin pumps and pacemakers to cars, toasters, and refrigerators will offer malicious hackers networked points of entry. Exploitation of social media networks and mobile devices will also grow. Crime will increasingly have a networked or cyber component.

Sketching the current and predicted landscape for cybercrime can lay the groundwork for exploring options to minimize the harmful influence of these markets. As part of ongoing studies on the future security environment, we examined these markets with support from Juniper Networks, a Silicon Valley manufacturer of networking equipment. Our findings could help private firms, public law enforcement agencies, and network security vendors gain a better understanding of the cybercriminal activity they aim to suppress. Without studying this activity and exploring the options to subdue it, very little is likely to change.

HACKER HEAVEN

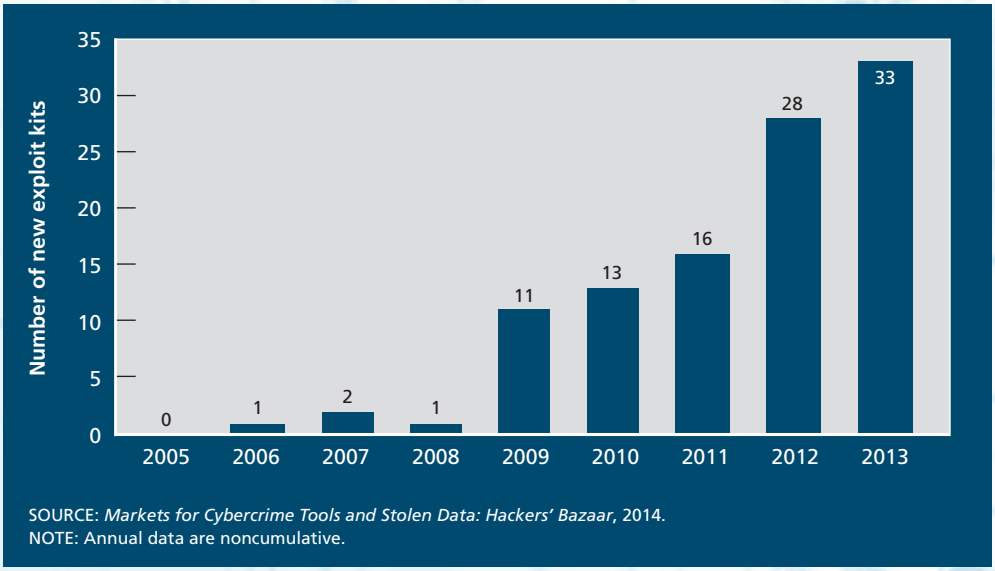
The black markets for cybercrime are a collection of activities that range from simple to extremely sophisticated and that operate all over the world, from New Jersey to Nigeria to China. There is no single location from which the markets emanate; a unique aspect of operating in cyberspace is that it is simultaneously nowhere specific yet everywhere. Goods and services are usually reliable. Implementation and transactions are quick and efficient. Cybercrime black markets are comparable to other underground markets for illicit goods, such as drugs, with the difference being that digital goods carry less risk and, for some, offer greater profit. Some organizations can make hundreds of millions of dollars per year.

The number of participants in cyber black markets is likely to rise, because it is easier to get involved than it was ten years ago. This is due to the proliferation of websites, forums, and chat channels where goods can be bought and sold. An increased number of YouTube videos and Google guides for "how to use exploit kit X" or "where to buy credit cards" also facilitates entry into the market, especially for buyers.

Figure 1 shows the proliferation of exploit kits over the past decade. Too numerous to name them all, the kits tend to go by feisty names such as Fiesta, Liberty, Lucky, Nuke, Siberia, Sploit, Tornado, Blackhole, Whitehole, Sweet Orange, and Cool. The price for kits varies based on whether they are purchased outright or rented. Do-it-yourself kits can cost as little as $15; high-end rentals can command $10,000 per month.

Originally, the major players in the cyber black market were former state employees of Eastern European countries who were well educated but found themselves searching for gainful employment after the Berlin Wall

Figure 1—Dozens of New Exploit Kits Expand the Cybercrime Market Each Year, While the Old Kits Remain in Use



SOURCE: *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, 2014.
NOTE: Annual data are noncumulative.

A unique aspect of operating in cyberspace is that it is simultaneously nowhere specific yet everywhere.

Glossary of Cybercrime

As-a-service: pertaining to outsourced hacking.

Botnet: a collection of compromised computers remotely controlled by a central authority to send out spam, spread malware, launch attacks, or support illegal websites.

Bug bounty: a reward given for finding and reporting a bug or vulnerability in a computer software product.

Cryptocurrency: a digital currency that incorporates codes and often offers anonymity.

Darknet: an anonymous private network that uses encryption and proxies to obfuscate who is communicating with whom.

Distributed denial of service: an attack by multiple compromised systems on a single system.

Encryption: the process of encoding messages or information in such a way that only authorized parties can read it.

Exploit kit: a tool that can be used to create, distribute, and manage malware to control user web traffic, infect users, or manage networks of infected machines.

Fraudware/fakeware: malicious software that poses as legitimate but is really not; it may falsely notify a user that a computer is infected with (other) malware.

Hacking: gaining access to a computer surreptitiously.

Malware: software intended to damage or disable computers or computer systems. Types of malware include viruses, worms, and Trojans.

Phishing: the attempt to capture usernames, passwords, and financial information by masquerading as a trustworthy entity using email or other electronic communications.

Rippers: people who do not provide the underground goods or services they advertise.

Spear-phishing: phishing attempts directed at specific individuals or companies.

Watering-hole attack: an attack on a popular website to infect all legitimate visitors.

Zero-day vulnerability: an exploitable vulnerability unknown to a software vendor and for which no patch has been created.

fell in 1989. Since then, the entrepreneurial savvy of the players has soared with the entry of a whole new generation of "digital natives" who can do more things for themselves. (They do not have to, for example, hire anyone to reverse-engineer a program or create an exploit.)

In terms of quantity, the leaders in malware attacks today operate out of China, Latin America, and Eastern Europe. In terms of quality, the leader is Russia. There are Vietnamese groups that focus on e-commerce, while a majority of Russian, Romanian, Lithuanian, Ukrainian, and other Eastern European groups focus on attacking financial institutions. Chinese hackers are believed to focus on seizing intellectual property, as underscored in May by the U.S. Department of Justice's accusations against five members of the Chinese military who have allegedly stolen trade secrets from five American companies and the United Steelworkers.

A stolen Twitter account now costs more than a stolen credit card, because a Twitter account potentially has a greater yield.

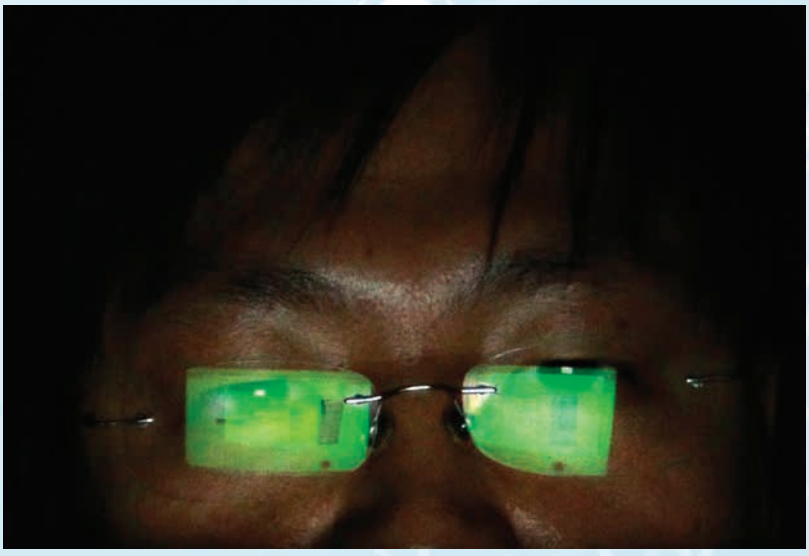
Some groups have partnered across international lines. As one expert put it, "Groups that would traditionally never work together are working together." One Vietnamese group partnered with Nigerians on a fraud scheme involving stolen e-commerce accounts. A Colombian group set up money-laundering "villages" in China.

U.S.-based participants in the market are becoming more involved. In 2007, the majority of participants were from Russia, with the United States having only a small representation. By 2013, almost a fifth of the market was U.S.-based, ranked third behind Ukraine and Romania.

Although English is the universal language of commerce, it is not necessarily the universal language of this commerce. The web forums are generally in Russian or Ukrainian. There are reports of English-only, Mandarin-only, German-only, and Vietnamese-only sites, among others. At the same time, the victim-deception campaigns of "phishing," "spear-phishing," and other social engineering operations are typically conducted in English, because a majority of the targeted victims know that language.

The product slate keeps evolving with the technology. Malware for mobile devices has been growing, in part because attacking mobile devices now brings in money faster than attacking personal computers. A stolen Twitter account now costs more than a stolen credit card, because a Twitter account potentially has a greater yield, for two reasons: A Twitter account can be used to target friends and family through spear-phishing schemes, and many unsuspecting consumers use the same password for their social media accounts as they do for their online banking and e-commerce accounts. Twitter is also becoming a channel of choice for the everyday transactions of malicious hackers, who are increasingly using private Twitter accounts to make deals rather than using open online forums or chat rooms.

Whatever is new or novel for the traditional consumer—from mobile devices to cloud computing to social media platforms—offers new entries for attack and will thus elicit a counterpart exploit on the black market. The trend will accelerate, because more and more of the world will have a digital component: By 2020, the number of connected devices will outnumber that of connected people by a ratio of 6:1, compared with about 3:1 today, doubling the avenues of potential exploitation.



REUTERS/PICHI CHUANG

A hacker works on his laptop in Taipei. Taiwan has become the front line in the global battle for cyberspace, according to hackers who describe the island as a rehearsal area for Chinese cyberattacks that are then directed toward larger countries.

RESILIENT TO ROUNDUPS

Law enforcement "takedowns" (or arrests) have had little effect on the size or composition of the black market. As one entity goes down, another takes its place, often within days. As the enduring entities implement countermeasures (such as stronger encryption, more vetting, and increased stealth), the market just hiccups, becoming somewhat less accessible and less open but mostly returning to normal. More of the market's transactions simply move to the "darknet"—that is, to anonymous private networks that use encryption and proxies to obfuscate who is communicating with whom. Illicit websites are also starting to accept only digital cryptocurrencies, with their anonymity, non-traceability, and other security advantages.

As one entity goes down, another takes its place, often within days.

The consequences of takedowns are transitory not only because of the market behaviors cited above but also because many countries condone hacker activity that is illegal in the United States. One Russian hacker was arrested, released on a technicality, given an apology, and now has ties to the government. China tends to turn a blind eye as well. On the other hand, Vietnam is very helpful to law enforcement groups, and Romania, Ukraine, and Poland have been selectively helpful.

Despite the transitory effects of cybercrime takedowns, they have recently been on the rise, for three reasons. First, law enforcement has gotten better over the past 10–15 years. Those entering the profession today have grown up comfortable with technology and computers, and training in the digital world has improved for law enforcers all over the world. Overseas partnerships and cross-pollination of ideas have also strengthened law enforcement—although perhaps more so at the federal level. Leadership in law enforcement, intelligence, and the U.S. Department of Defense has accorded cybercrime top priority and moved resources accordingly.

Second, suspects are going after bigger targets and thus are attracting more attention. Since around 2002, attacks have shifted from opportunistic one-offs (against whichever individuals may have been unsecure) to companies. Now that companies understand they are targets, they are more willing to work with law enforcement, and the public-private partnership has tightened.

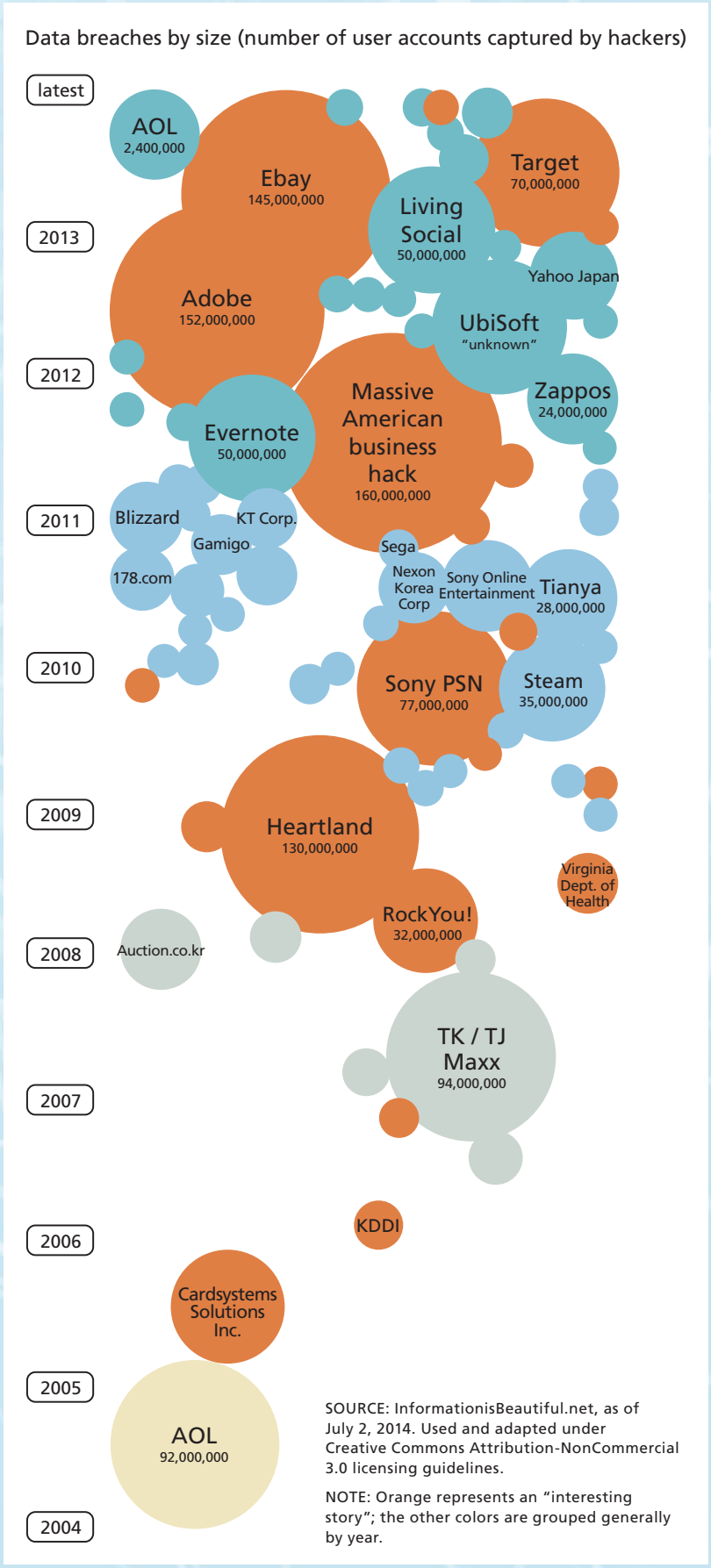
Third, because almost every aspect of crime today involves a digital component, law enforcement has a multitude of opportunities to encounter crime in cyberspace and to learn from these encounters. (Figure 2 illustrates the biggest data breaches in history as a result of malicious hacking.)

However, as mentioned above, law enforcement could also become a victim of its own success. More arrests and takedowns lead to more media coverage, drawing more perpetrators into the black markets and compelling those already in the markets to grow smarter.

QUICKER ON THE DRAW

Today, malicious hackers appear to have the upper hand. The maturation of cybercrime markets threatens individuals, businesses, law enforcement agencies, national governments, and military services around the world. The deleterious effects on cybersecu-

Figure 2—Data Breaches Show No Sign of Letting Up



SOURCE: InformationisBeautiful.net, as of July 2, 2014. Used and adapted under Creative Commons Attribution-NonCommercial 3.0 licensing guidelines.

NOTE: Orange represents an "interesting story"; the other colors are grouped generally by year.

REUTERS/JASON REDMOND

Vishant Patel, of the Microsoft Digital Crimes Unit in Redmond, Washington, shows a heat map illustrating the proliferation of attacks from malicious networks, known as botnets, on computers in Western Europe.

rity suggest the need for coordinated efforts across the private and public sectors, nationally and internationally, to suppress the black market activity.

In the private sector, computer security companies, device manufacturers, Internet service providers, and defense contractors should routinely collaborate on developing updated approaches to thwarting online attacks. Beyond the technical solutions (such as ever-thicker firewalls and ever-stricter access controls), there are intriguing possibilities for private firms to harness the power of their legitimate markets to fight illegitimate ones.

For example, more private firms could sponsor "bug bounty" programs or related contests, which offer financial rewards to anyone who finds or reports a bug, virus, or other vulnerability in a particular computer software product. Google's bounty program pays $3,000 to $5,000 for ordinary, easier-to-find bugs, with bounties in the range of $20,000 or even upward of $200,000 or more for exotic and exceptionally nefarious bugs, or those that affect a large market segment. The U.S. government could funnel money to security vendors to help with their bug bounty programs, or even create its own. As for computer hacking contests, one good example is the annual Pwn2Own competition, which began in 2007 and paid out $850,000 of prize money in 2014.

Commercial companies, defense contractors, and government agencies alike could also offer better pay and incentives to lure talented hackers away from the illicit markets and into legitimate business and government operations (especially those targeting the activities of other hackers). All of these strategies could work in tandem: The bug bounty programs and recurrent contests could serve as recruiting programs for permanent hires. With better pay and incentive packages, the savviest hackers would gravitate toward legitimate work, and the private firms and government agencies would reap the benefits while removing the dangers. Over time, this approach might even stop the arms race between security vendors and those trying to render their products obsolete.

When hackers succeed in stealing customer data and placing the data on the open market, banks or other mer-

Commercial companies, defense contractors, and government agencies could offer better pay and incentives to lure talented hackers away from the illicit markets.

chants could possibly buy back their customers' stolen information. This strategy would raise valid ethical questions about legitimate businesses participating in the black market for the implicit purpose of paying "ransom" for data "hostages." But if the information is already stolen, this strategy might be a viable way to protect it. On the other hand, this strategy could backfire by alerting the attackers to what merchants believe is most important, or most vulnerable, thereby bidding up the price for this particular kind of stolen data and enticing the thieves to seize even more.

Law enforcement agencies could pursue several strategies, some of which would benefit from advice from computer security firms. For instance, law enforcement agencies could explore the costs and benefits of establishing fake credit card shops, fake forums, fake websites, or other cyber sting operations to boost the number and quality of arrests, while simultaneously tarnishing the reputation and confidence of the black markets. These agencies could also explore the ramifications of hacking back—or including an offensive component within law enforcement—to deny, degrade, or disrupt black market business operations. The lessons learned from infiltrating, disrupting, and combating the black markets for illegal drugs and illegal arms could also be applied to the black markets for cybercrime.

Law enforcement and other government agencies could perhaps use the black market to their advantage in their own offensive operations: By using black market cyber goods, such as exploit kits and encryption tools, a government officer would appear online as just another criminal, would not stand out, and would reduce the risk of being "fingerprinted." Public opinion could collapse, however, if word got out that the U.S. government were involved in the black market. Therefore, this tactic might be allowed for only highly sensitive operations or extremely targeted attacks.

Law enforcement agencies will also need to determine whether it is more effective to pursue the small number of top-tier cybercriminals or the large number of lower-tier participants. Worldwide, law enforcement agencies will need to work together to prosecute and extradite the most wanted criminals, coordinating their arrests and indictments.

From a regulatory standpoint, both private companies and law enforcement agencies should inform legislators about the costs and benefits of implementing various potential mandates: for encryption on point-of-sale terminals (cash registers and online shopping carts), for safer storage of passwords and user credentials, for worldwide adoption of credit cards with embedded computer chips and personal identification numbers, and for regular checks of websites to prevent common vulnerabilities. All such mandates would be intended to put a dent in the black market or to force major changes in how it operates.

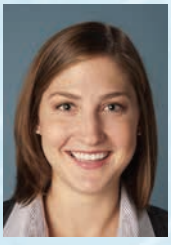
The urgency of these strategies will grow over time. In their absence, not only will very little likely change to deter the criminals, but the victims will stand to lose more and more. ■

RELATED READING

Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar, Lillian Ablon, Martin C. Libicki, Andrea Golay, RR-610-JNI, 2014, 81 pp., web-only, www.rand.org/t/RR610

PHOTO CREDITS: GENERAL STORE ON PAGE 12: ©ISTOCK.COM/BCFC; CYBER SKY ON PAGES 12–19: ©ISTOCK.COM/NADDI; MONITOR ON PAGE 15: IMAGE VIA SAMSONOVS/FOTOLIA

Law enforcement agencies could explore the costs and benefits of establishing fake credit card shops, fake forums, fake websites, or other cyber sting operations.



Lillian Ablon is an information systems analyst focusing on both the technical and human aspects of cybersecurity at the RAND Corporation. Martin C. Libicki is a senior management scientist at the RAND Corporation.

From Azerbaijan to Zambia:

One of the principal goals of U.S. "security cooperation" with other countries is to reduce their fragility. In pursuit of this goal, security cooperation relies heavily on U.S. assistance to the internal and external security organizations of countries around the world. But does the strategy work? RAND researchers analyzed more than 100 countries that had received U.S. security cooperation assistance from 1991 to 2008, including such major recipients as Colombia, Jordan, the

Many Types of Soil

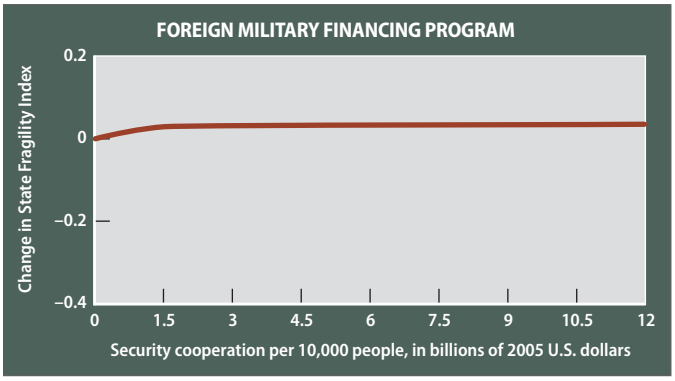
The darker the country on the map, the stronger the likelihood that its stability will improve with U.S. security cooperation. The more developed, less fragile states in Latin America, Europe, and much of Southeast Asia offer the most hospitable terrain. The prospects are less promising in much of Africa and in central Asia because of the prevalence of authoritarian regimes, lower state capacity, and higher levels of fragility (based on security, economic, political, and social conditions). This does not mean that such states should be starved of U.S. security cooperation, but it does mean that the expectations should be lowered commensurately.

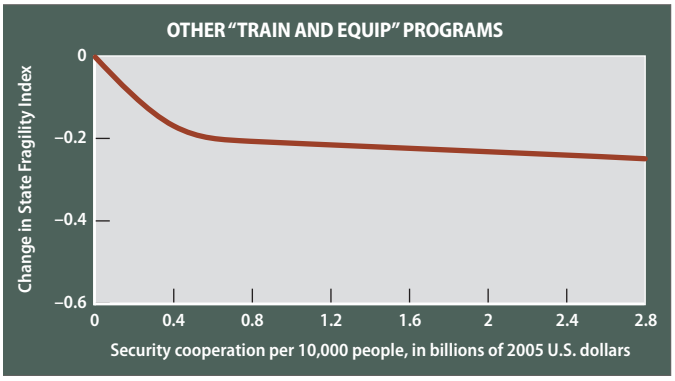
Four Types of Seeds

The extent of success may depend also on the type of security cooperation. The four graphs below show how different types of aid correlate with changes in state fragility; a lower score suggests reduced fragility. The Foreign Military Financing Program, which provides equipment-based aid, has not correlated with reduced fragility—possibly because such aid is often geared toward other goals. However, other "train and equip" programs (such as counterterrorism), professional military education funding, and counternarcotics and law enforcement funding have all correlated with drops in fragility. Given the relatively low cost of military education funding in particular, investing in the human capital of partner security forces may yield the greatest return in terms of reducing state fragility.

Productive Global Stewardship

On the whole, U.S. security cooperation appears to make real contributions toward reducing fragility in partner countries, especially at the lower end of the cost spectrum. Substantially larger investments have not produced proportional drops in fragility. The U.S. Army's increased focus on security cooperation is in accordance with these results, as is a growing emphasis on small-footprint efforts by special operations forces to cultivate partner capacity.

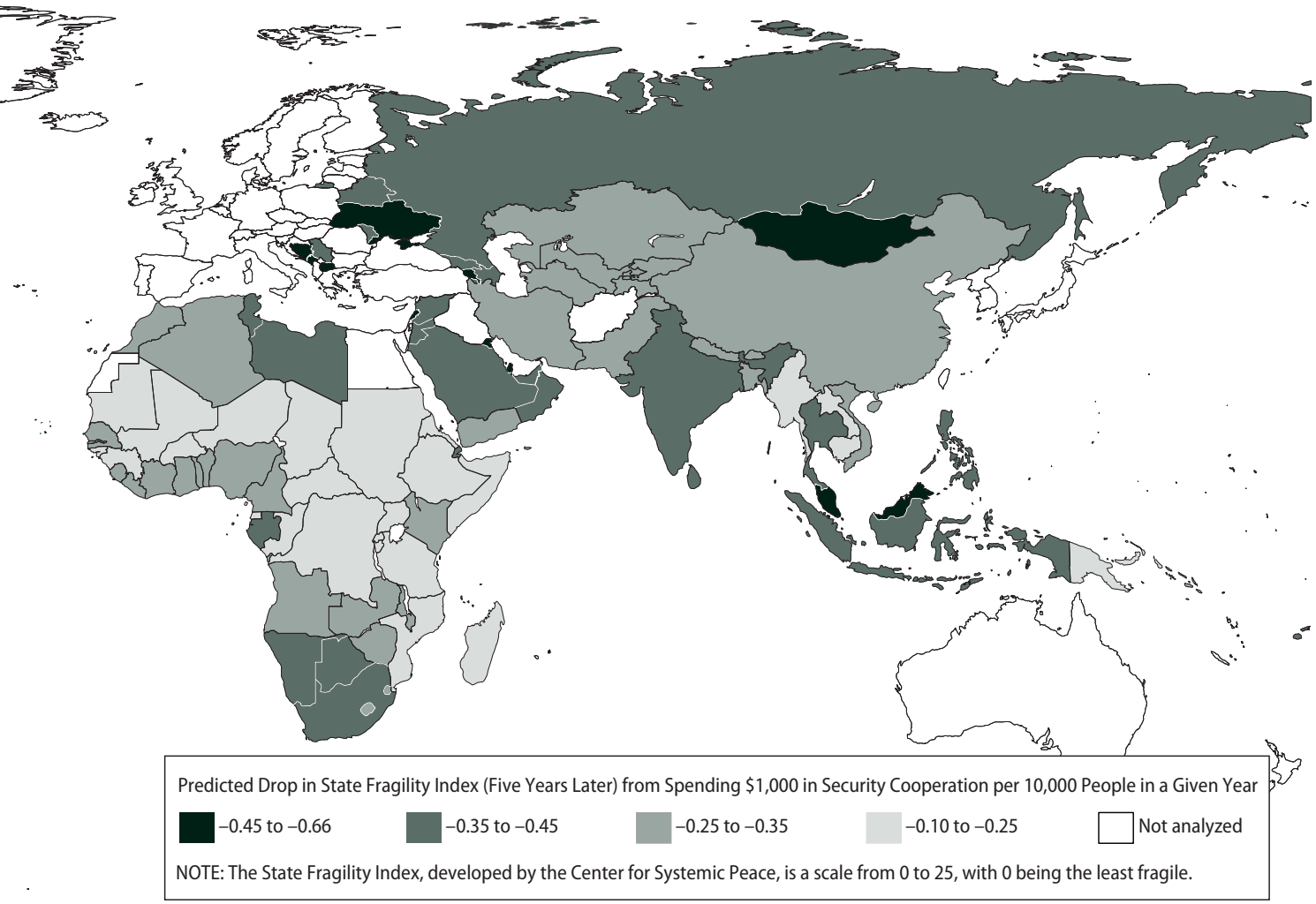


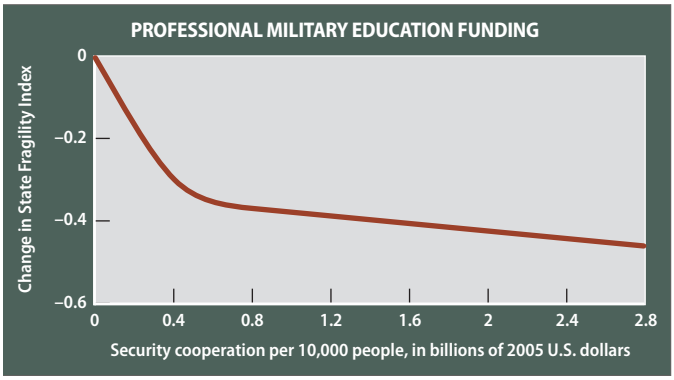


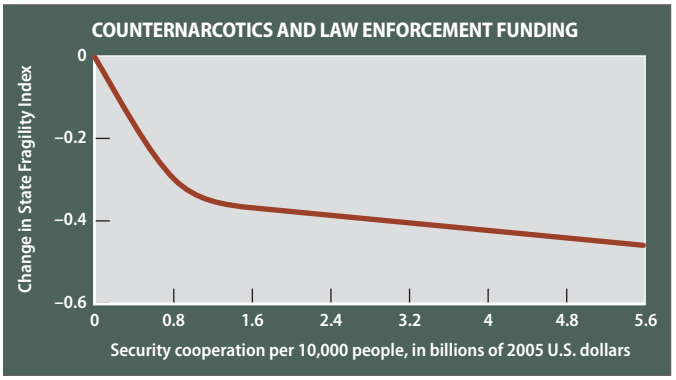
SOURCE: *Assessing Security Cooperation as a Preventive Tool*, Michael J. McNerney, Angela O'Mahony, Thomas S. Szayna, Derek Eaton, Caroline Baxter, Colin P. Clarke, Emma Cutrufello, Michael McGee, Heather Peterson, Leslie Adrienne Payne, Calin Trenkov-Wermuth, RR-350-A, 2014, 150 pp., www.rand.org/t/RR350

Security Cooperation Bears Fruit, Depending on the Type of Soil and the Type of Seeds

Philippines, Uganda, and Yemen. The researchers found that, on average, security cooperation did correlate with a statistically significant reduction in state fragility within five years. The effect was weakest in countries that were less democratic and most at risk of state failure. This suggests that security cooperation might be better at reinforcing success than in halting a country's decline into instability—all of which underscores the importance of prevention as a form of security cultivation.







NOTE: Lines on the four graphs show best estimates; 90-percent confidence intervals (not shown) straddle the lines but fall entirely below zero in the final three graphs.

The Telescope and the Microscope

Public Policy Wisdom from Victor Hugo

By Michael D. Rich

Michael D. Rich, president and chief executive officer of the RAND Corporation, made the following remarks at the Pardee RAND Graduate School Commencement Ceremony in Santa Monica, California, on June 21, 2014.

FOR 55 YEARS, RAND HAS PUBLISHED AN ANNUAL calendar with inspirational quotations. I hope many of you noticed the quotation for April in the 2014 calendar. It happens to be my favorite line from *Les Misérables*. I am sorry to say that the line didn't make it into the musical or the film; it's only in the book. It comes in the section of the story when Jean Valjean and Cosette are living incognito in Paris. Victor Hugo wrote an entire chapter about the overgrown garden on their compound that served to conceal their houses. The chapter includes a very detailed passage about the interconnectedness of nature. It is fascinating to read, but what caught my eye about halfway through the chapter were this statement and question:

"Where the telescope ends, the microscope begins. Which of the two has the grander view?"

Hugo leaves that question unanswered, hoping, I am sure, to get readers like me to ponder it. I like the question because I think it has deep meaning for policy analysis, particularly the kind invented and practiced here at RAND.

So, which has the grander view? Both reveal truths that are not observable with the ordinary eye. The telescope enables us to see far into the distance, beyond our immediate horizons, and beyond our reach. The microscope enables us to look deeply, closely, to reveal the hidden workings of what's all around us. Both often show that what might, at first, seem obvious or simple is anything but that.

Much of what you have learned in the Pardee RAND classrooms probably seemed like looking through a microscope. You've learned how to use advanced data collection techniques, statistics and economic modeling, complex computer simulations, rigorous case studies, and a lot more. Those are tools we use to unpack trends, distinguish correlation from causation, surface latent opportunities for savings, and reveal hidden costs. You've learned how to use those tools to dissect policies and programs—breaking apart systems into essential elements, searching for the factors that matter most in producing desirable outcomes, devising ways to reconfigure the pieces to produce a more effective or efficient whole.

But, because you've been a part of RAND, I hope you've also had a view through the telescope. I hope you have lifted your head from the focused field of the microscope to look up and to look out, in order to explore the larger context in which today's discrete challenges reside, take the long view, and think about society's largest challenges, even when—and perhaps especially when—those challenges are too big, too complex, and seemingly too distant to be on current policy agendas.

So which has the grander view—is it the microscope or the telescope? My answer is that for a policy analyst, the grandest view is achieved by embracing them both. Your experience in two interlocking institutions, the Pardee RAND Graduate School and the RAND Corporation, has served you well in this regard.

I am afraid that the policy problems you will tackle in your careers will be more challenging than the ones I have addressed in mine. The world is more complex than ever, and there are many factors with potential to make it even more dangerous.

My wife and I just became grandparents for the first time, so we have a brand new stake in the future. Naturally, we want a world in which people are healthier, safer, more secure, and more prosperous. We are counting on you to see the biggest problems first, to create bold solutions that work, and, most important of all, to see them through. In my judgment, you can best accomplish this by using both a telescope and a microscope. ■

Both reveal truths that are not observable with the ordinary eye. Both often show that what might, at first, seem obvious or simple is anything but that.

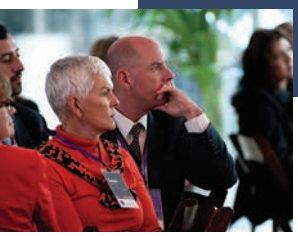
November 13–14, 2014
Santa Monica, California

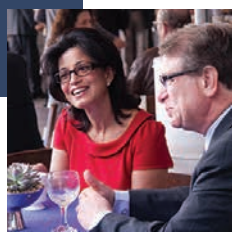
Set Politics Aside and join the conversation.

"Politics Aside is not an event with stump speeches and ideological rhetoric. RAND invites the audience to become part of a substantive and thought-provoking exchange.

This is something you just don't get anywhere else."

Michael Lynton, *CEO, Sony Entertainment, Inc.; Chairman and CEO, Sony Pictures Entertainment*





Politics Aside is a postelection event that engages policymakers, opinion leaders, philanthropists, and RAND's leading thinkers in a nonpartisan examination of pressing policy challenges.

Find out who's coming, what's happening, and how to sign up for passes and updates.
www.rand.org/politicsaside

If you have questions or would like to become a sponsor, contact us at
politicsaside@rand.org, or call **1-800-757-4618**.

RAND CORPORATION with media partner THOMSON REUTERS

RAND

HEADQUARTERS CAMPUS
1776 MAIN STREET, P.O. BOX 2138
SANTA MONICA, CA 90407-2138

OFFICES
SANTA MONICA, CA
WASHINGTON, DC
PITTSBURGH, PA
NEW ORLEANS, LA
JACKSON, MS
BOSTON, MA

CAMBRIDGE, UK
BRUSSELS, BE

NON-PROFIT ORG.
U.S. POSTAGE
PAID
THE RAND
CORPORATION

INVESTING IN PEOPLE AND IDEAS

"It's important for a research institution to be independent and able to say to its clients—and for that matter, its donors—'We will be honest agents.' I invest in RAND because I believe that research and knowledge is the basis of any social change, that we need objective, evidence-based research to advance public thinking and public policy. RAND does that, and that's really at the heart of why RAND is so credible and so important."

Faye Wattleton is a managing director with Alvarez & Marsal, a leading independent global professional services firm, and a member of the Pardee RAND Graduate School Board of Governors.

Generous contributions from donors such as FAYE WATTLETON enable RAND, a nonprofit organization, to fund groundbreaking research in the public interest.

CP-22-1408