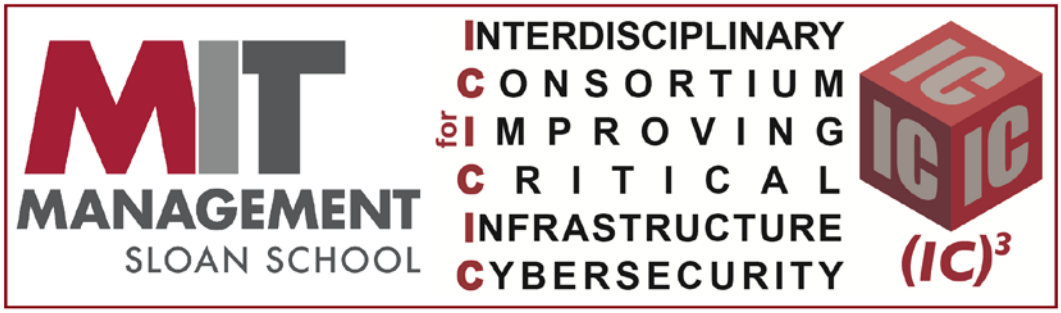


Battling Cybercrime: MIT Tackles a Global Challenge

Alix Stuart

Working Paper CISL# 2017-08

May 2017

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Summer 2017

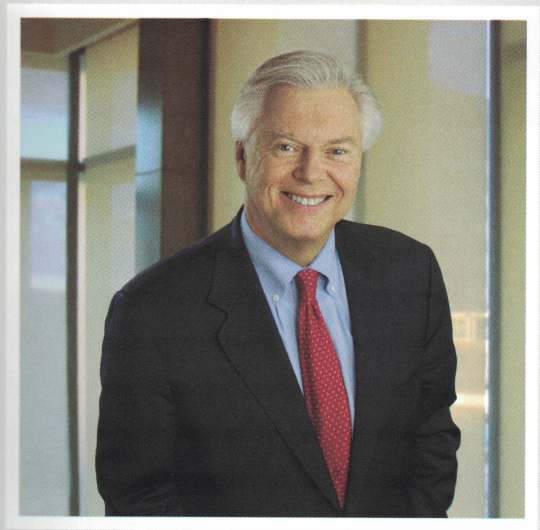
News and insights for the MIT Sloan community

MIT SLOAN

BATTLING CYBERCRIME

MIT TACKLES A GLOBAL CHALLENGE

DEAR FRIENDS,



At MIT Sloan, we are proud to be MIT's school of management. Studying and teaching management in our uniquely MIT way means that we work together to solve complex problems. We look beyond traditional boundaries and work across disciplines, forming partnerships across campus and with industry to tackle some of the world's most pressing challenges.

In this issue of *MIT Sloan*, we showcase two current examples of such creative collaboration. Our "Innovation at Work" article explores the research of an interdisciplinary team of faculty led by Retsef Levi and Yasheng Huang. Their goal? To make the global food supply chain more secure by developing models to better predict and prevent risks to food safety.

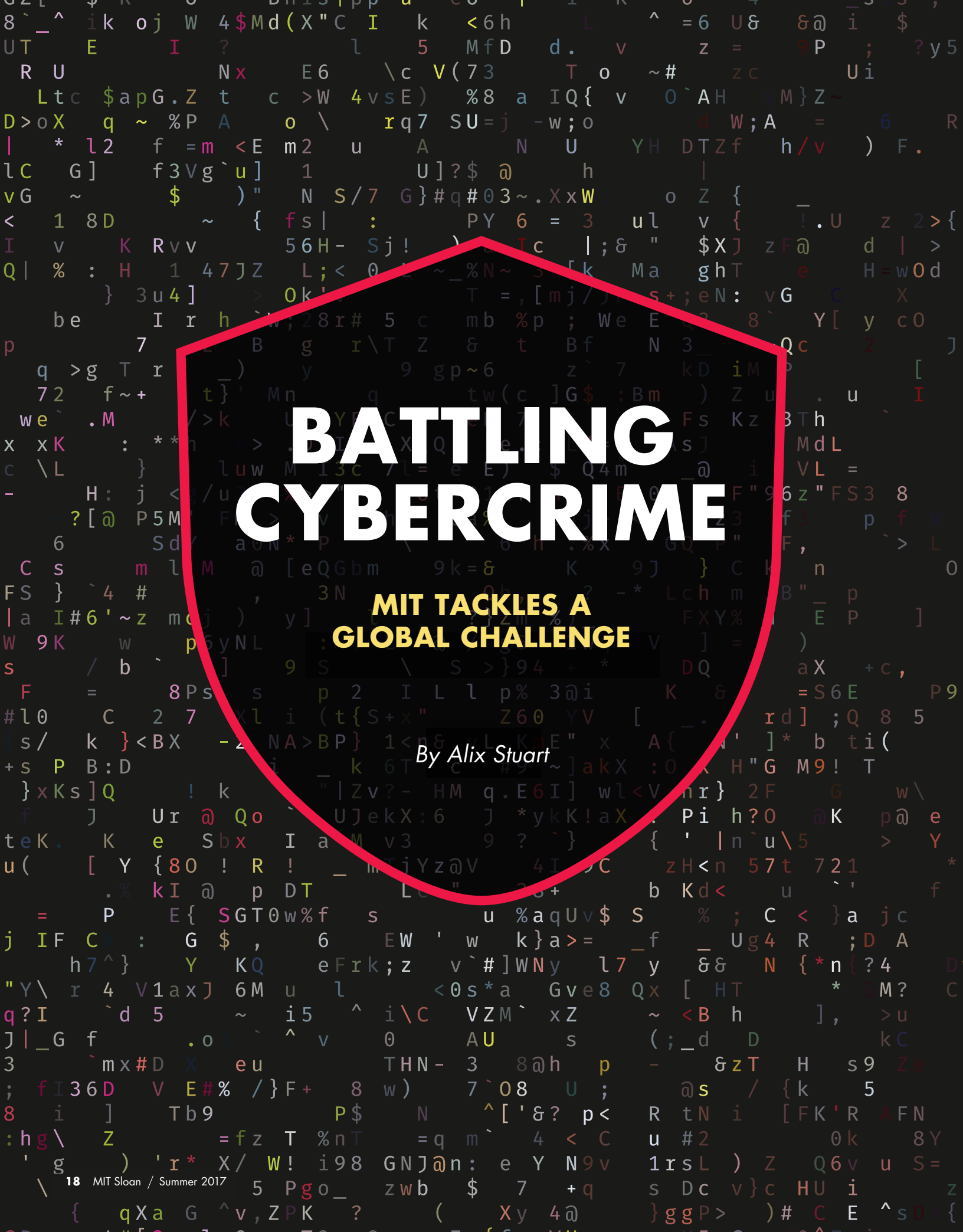
Our feature article, "Battling Cybercrime," looks at how the school's Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity—dubbed $(IC)^3$—has assembled a cross-Institute team to explore the technical, trade, policy, and managerial implications of cyberattacks. Led by Stuart Madnick, $(IC)^3$ is working with several teams to explore how better information and a more holistic approach to preventing cyberattacks can help businesses and governments both anticipate and recover from data breaches.

These are just two examples of the critical problems that are especially well-suited to being solved at MIT—where some of the world's brightest minds come together to invent solutions to improve the world.

Sincerely,

David Schmittlein

David Schmittlein
John C Head III Dean



BATTLING CYBERCRIME

MIT TACKLES A GLOBAL CHALLENGE

By Alix Stuart

Cybersecurity is a topic that regularly frustrates executives and government officials. They spend inordinate time and worry trying to protect their data, yet on balance, it's a losing battle. Nearly two-thirds of Americans say they've had digitized personal information stolen, according to a recent survey by Pew Research Center, and few have confidence in companies or the federal government to protect them.

Sophisticated phishing schemes, ransomware, state-sponsored hacking, and the like certainly contribute to this maddening struggle. But at the heart of the problem is a simple fact: "People tend to think cybersecurity is solely a technology problem," says MIT Sloan's Stuart Madnick, the John Norris Maguire (1960) Professor of Information Technology and academic director of MIT Sloan's Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, also known as (IC)³.

Instead, "cybersecurity issues are multi-faceted, much like a multi-headed hydra," says Madnick, "so they need to be addressed in a multi-disciplinary manner—which is one of MIT's great strengths." Consider a ransomware attack that effectively locks up an organization's data and systems. On the surface, this problem—which many hospitals have faced in the past year—is a technical one: Can the data be unlocked, and how fast? But embedded within it is a host of management problems, as well, including decisions about whether to pay the ransom, how the organization should operate if its data remains locked, and whether new policies are required to respond to similar issues in the future.

To achieve a more holistic approach on cybersecurity, Madnick and other MIT Sloan faculty are increasingly collaborating internally and across the MIT campus, with the goal of getting ahead of the real-world problems that keep executives and political leaders up at night. Research topics range from the governance of the internet to global trade policies for cyber-risky internet-enabled devices to new approaches for calculating the costs and benefits of cybersecurity investments.

"Cybersecurity has technical, trade, and policy implications, along with the managerial ones. If you can't bring together all those forces, you can only launch a partial attack," says Madnick.

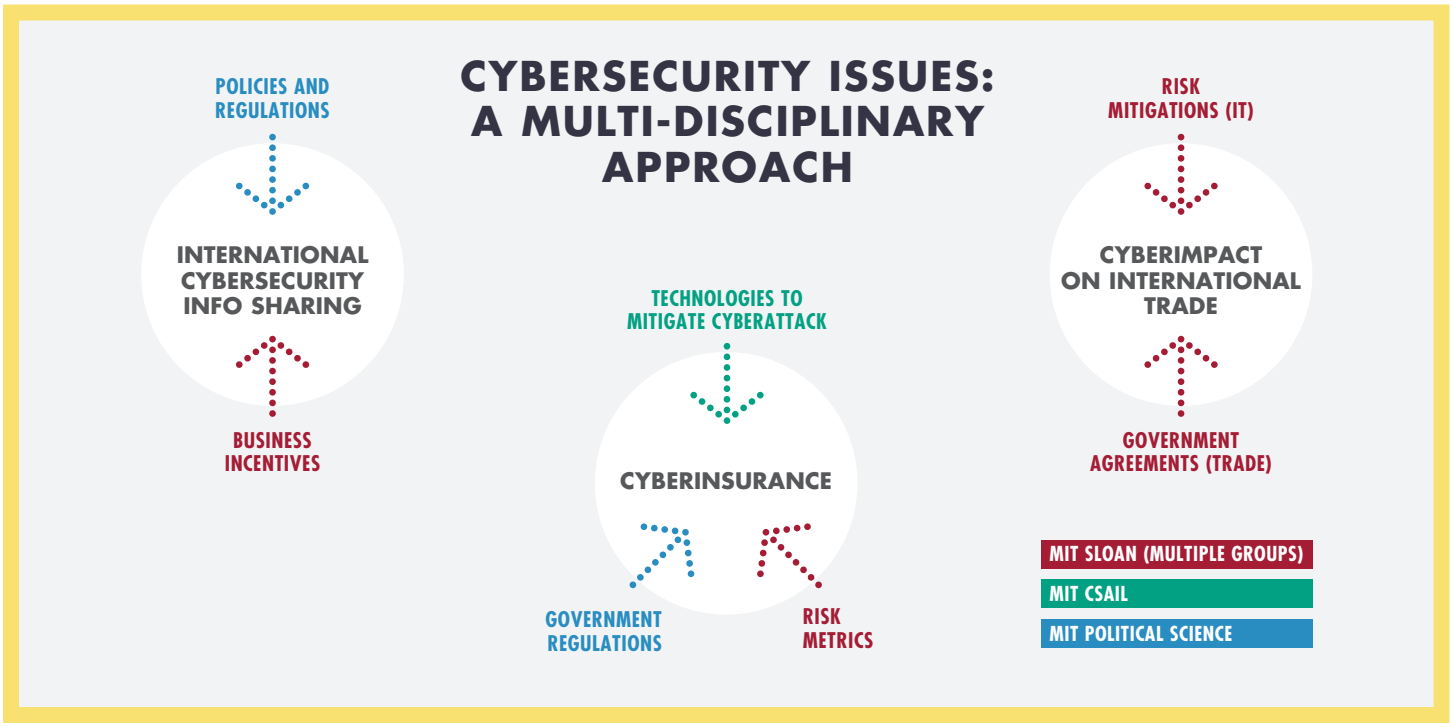
And MIT Sloan is exactly the right place to combine such forces. With a rich history of collaboration across the campus, "the ability to bring world-class technology and engineering resources to address managerial problems is unparalleled," says Madnick. Plus, cybersecurity is increasingly rising to the level of being the type of "really hard problem" that MIT exists to overcome. "This sits right in the center of our mission to make the world a better and safer place."

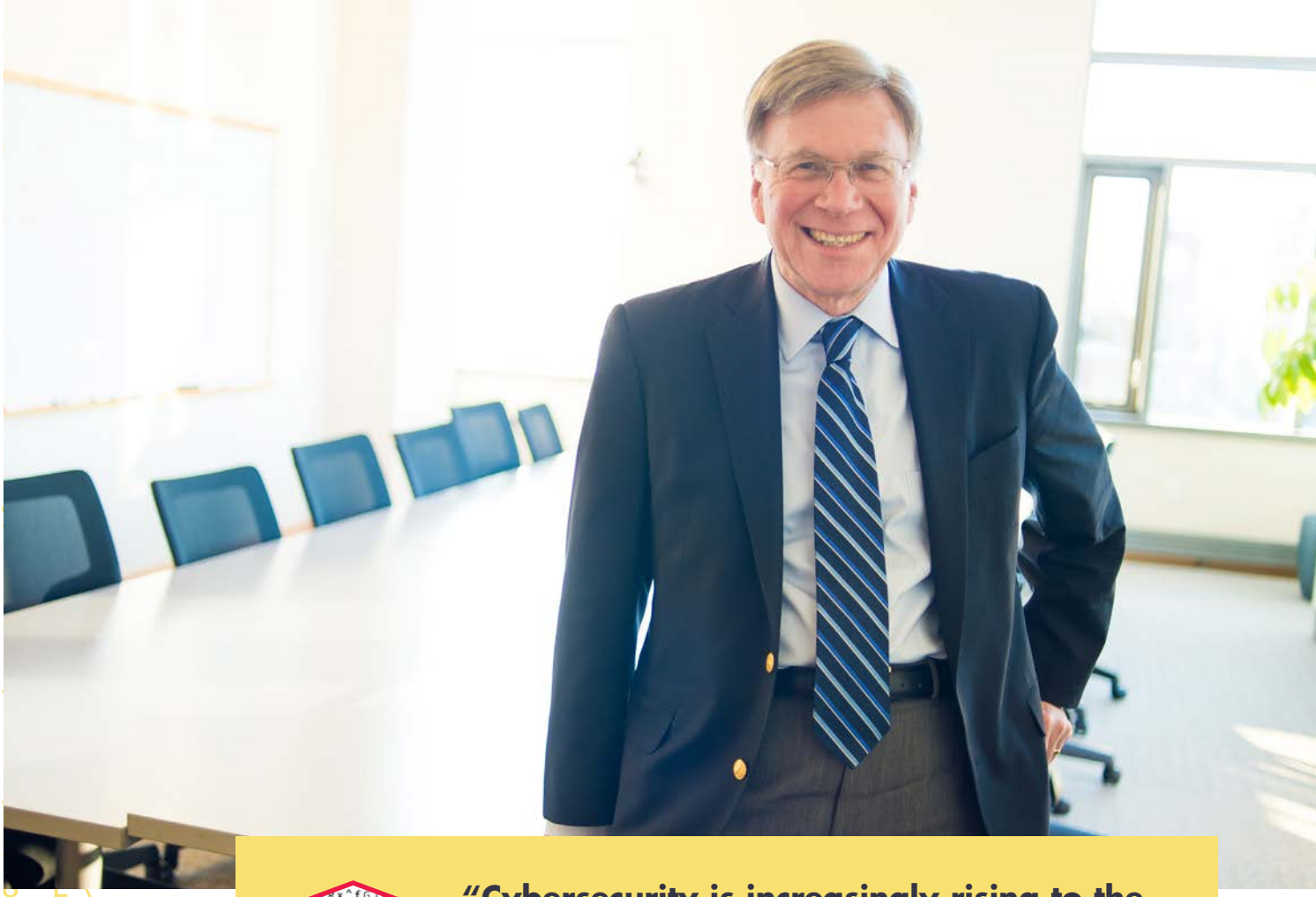
WHO'S THE BOSS?

A big question anchoring a major strand of MIT Sloan research collaboration is: Who exactly is in charge of cyberspace? Who is policing its borders, and who is to blame when things go wrong? While each country may have its own policies and governance for the internet, there is little coordination among them. And many elements of cyberspace transcend existing country borders: The undersea cables that carry nearly all internet traffic crisscross the globe, for example.

"Existing law is attached to countries, but the internet is not just about countries," notes Nazli Choucri, an MIT professor of political science, who is currently working with Madnick to examine what new structures or rules the boundless world of cyberspace might require. In her view, cyberspace will require a new set of laws, as well as new transnational institutions to govern it. And that has major implications for company decision making, since "country-level issues and consequences are inexorably woven with company-level issues and consequences," says Madnick.

So far, though, countries don't typically even share information about when or how often they've been hacked, much less discuss how to band together against such attacks. "Often, we don't agree





"Cybersecurity is increasingly rising to the level of being the type of 'really hard problem' that MIT exists to overcome."

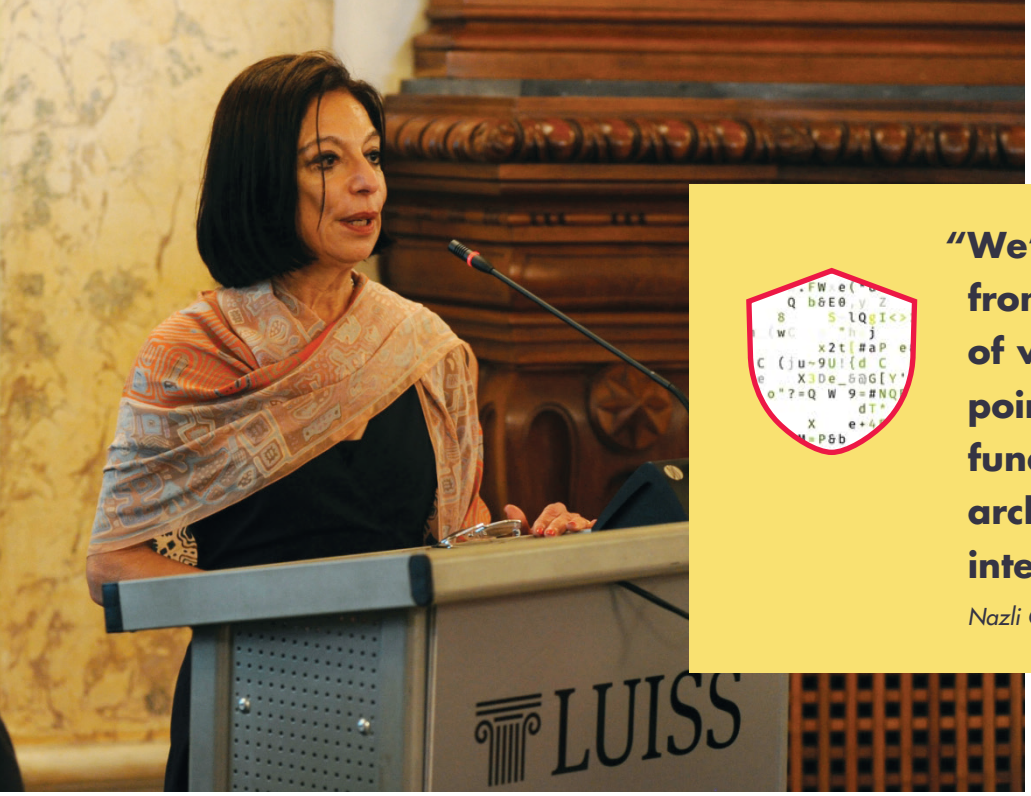
Stuart Madnick, John Norris Maguire (1960) Professor of Information Technology

across countries on how to define cybersecurity or incidences of cyberattacks," Choucri says. "On the obvious issues, governments across the world do not willingly share information, and neither do international institutions that are presumably above the fray."

That's the bad news. But Choucri's work with Madnick seeks to catalogue existing practices and move forward with a framework and standards that would make it easier for sharing to occur. Improving cybersecurity information sharing will actually improve cybersecurity, their research proposal notes. "We are seriously lagging in basic interaction," says Choucri. "As a result, we may be creating serious opportunity costs—for all."

In hopes of broadening the perspectives of the next generation of leaders, Choucri and Madnick co-taught a cybersecurity course last semester that featured a variety of guest speakers, such as researchers from the MIT Center for International Studies within the Political Science department and the Internet Policy Research Initiative (IPRI) and Cybersecurity@CSAIL; an initiative within the Computer Science and Artificial Intelligence Lab (see sidebar on page 24). This course was cross-listed in both MIT Sloan and the Political Science department. "We're teaching cybersecurity from both a geopolitical point of view and from a business point of view, then including fundamentals like the architecture of the current internet," says Choucri. "Those three sides are all closely interwoven; you really can't untangle them."

Meanwhile, IPRI is a cross-MIT research initiative that is examining related themes. "Our goal at IPRI is to develop technically grounded internet public policy options for governments around the world," says IPRI founding director Daniel J. Weitzner, former U.S. Deputy Chief Technology Officer for Internet Policy in the White House. With faculty leadership from MIT Sloan



"We're teaching cybersecurity from both a geopolitical point of view and from a business point of view, then including fundamentals like the architecture of the current internet."

Nazli Choucri, MIT Professor of Political Science

as well as departments such as Political Science, EECS, Sociology, and Anthropology, research in IPRI spans policy aspects of encryption, protecting critical infrastructure, privacy, network architecture, and machine understanding. Related materials, in particular case studies that explored the questions arising from the conflict between Apple and the FBI over access, were used in MIT Sloan's module of ethics of cybersecurity.

EYES EVERYWHERE

Against the backdrop of such a big-picture, systemic investigation into the internet, an emerging project within MIT Sloan is looking at what it means to have the power of the internet embedded in small devices throughout our lives.

The Internet of Things—the catchphrase for the rapidly growing class of internet-enabled devices such as smart TVs and self-driving cars—is largely known for its convenience factor. According to leading economist Simon Johnson, PhD '89, however, it is a threat to global trade and national security. Together with Madnick, Johnson—the Ronald A. Kurtz (1954) Professor of Entrepreneurship and professor of global economics and management at MIT Sloan—is investigating how governments are and should handle imports of items that could ultimately be a conduit for harming their citizens.

While it may sound far-fetched, some governments are already dealing with such concerns. Since 2012, for example, the U.S. Congress has urged U.S. telecommunications companies not to purchase network equipment from two Chinese companies, Huawei and XTE, for fear that the hardware could funnel intelligence back to China. On the flip side, this year Germany banned an interactive toy made by U.S.-based Genesis Toys, My Friend Cayla, on the grounds that the doll's internal camera could be used to spy on its citizens.

"These are harbingers," said Johnson, of a scenario in which countries, by attempting to block the potential for international spying via internet-enabled devices, could force global trade to grind to a halt. That's because as the scope of products with internet connections extend to such common items as toothbrushes, such restrictions could effectively cover the majority of products—except perhaps bricks, Madnick remarks.

While the research is still in its formative stages, one of the project's aims is to create a framework that policymakers could use in constructing treaties with foreign governments. For governments, "the question is who trusts us and whom do we trust, in terms of what may be embedded in electronics—or really anything that has any kind of electrical element," says Johnson. The follow-on question is "Can you converge on some type of standards?" so that trade can continue flowing despite the malicious potential of some items.

Johnson and Madnick are hoping that large multinational companies will play a prominent role in the research, and welcome feedback from them. A major open question is whether standards should cover companies as entities or simply individual product lines. "If you trust Apple, does that mean anything they produce is fine?" Johnson asks. Companies will also have to decide how to respond to the fact that governments appear increasingly

able to work around their security measures in order to, say, unlock phones of those involved in crimes, or listen in on cellphone conversations for signs of suspicious behavior.

NEW MATH, TIMELESS PROBLEMS

Yet another dimension of narrow thinking around cybersecurity is the impulse to underinvest in defensive measures, since it's difficult to measure how effective any given level of spending is. "There are about 100 well-known ways you can improve your cybersecurity, and if everyone did all of them, we'd probably improve quite a bit," says Jerrold Grochow, an MIT Sloan PhD who was formerly MIT's vice president of information systems and technology, and is now a research affiliate with MIT Sloan and the (IC)³ initiative. "The problem is that these measures cost money, and it's not a one-time thing; you have to constantly maintain them."

Grochow is now working on an economic model that would make such management decisions more straightforward. "We're unlikely to get to something as simple as a return-on-investment calculation that people can specify with absolute certainty, but I think we can get to some calculations that say, "If you think a cyber event is no more or less likely to happen every N years, then you should be spending X amount of money because the payoff is Y," he says.

continued on page 25

"The question is who trusts us and whom do we trust, in terms of what may be embedded in electronics—or really anything that has any kind of electrical element."

Simon Johnson, PhD '89, Ronald A. Kurtz (1954) Professor of Entrepreneurship and Professor of Global Economics and Management

(From left) S.P. Kothari, Howard Shrobe, President L. Rafael Reif, Daniela Rus, Maria Zuber, Daniel Weitzner, Stuart Madnick, and Director of MIT Lincoln Laboratory Eric Evans

Cybersecurity@MIT: A Three-Legged Stool

Anticipating the constantly increasing threats posed by cybersecurity, in March 2015, MIT officially announced the Cybersecurity@MIT Initiative. It consists of three interrelated multidisciplinary cybersecurity research efforts: Cybersecurity@CSAIL, focused on improved hardware and software; the Internet Policy Research Initiative (IPRI), focused on policy; and the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, (IC)³, focused on the managerial, organizational, and strategic aspects of cybersecurity.

At the kickoff event, MIT President L. Rafael Reif emphasized both the new initiatives' partnerships with industry and the interdependence of the research programs. "New technologies will require new policies and incentives," he said. "Emerging policies must adapt to future technologies. And none of that matters if they cannot make the present a safe place to do business."

The IPRI works directly with policymakers and technologists to help solve problems. Led by former U.S. Deputy Chief Technology Officer for Internet Policy in the White House Daniel Weitzner, as well as faculty researchers from engineering, social science, and management labs at MIT, the center recently published a set of presidential-level policy recommendations based on a two-year analysis of critical energy, finance, and communications systems in the United States. A past report on encryption policy, "Keys Under Doormats," was a key input to the FBI/Apple encryption debate, and led to the report's authors testifying before the U.S. Congress four times. Many of the IPRI projects have co-principal investigators from two or even three different departments including MIT Sloan, reflecting the interdisciplinary aspect of cybersecurity policy.

The Computer Science and Artificial Intelligence Laboratory (CSAIL), the largest lab on campus, was created by the merger of two predecessor labs that date back to the 1950s—one was the Laboratory for Computer Science (LCS), where the first user IDs and passwords were introduced, and where Madnick received his PhD. CSAIL has long been at the forefront of internet and security issues, from developing large parts of the internet architecture to creating data encryption systems. It is home to the World Wide Web Consortium (W3C), directed by Tim Berners-Lee, inventor of the web.

While it often takes years to move from research to commercially available products, CSAIL has already helped some promising startups in the cybersecurity field get off the ground. In 2016, for example, the startup PatternEx launched its first service offerings, based largely on CSAIL research that combined human input with artificial intelligence to predict cyberattacks about three times more accurately than previously existing products. PatternEx co-founder Kalyan Veeramachaneni launched it as a research scientist at CSAIL with Una-May O'Reilly's research group AnyScale Learning For All (ALFA); the company's chief data scientist, Ignacio Arnaldo, is a former ALFA and CSAIL post-doc.

Besides the differences in research focus, each of the three programs has its own unique operational model. Cybersecurity@CSAIL is currently sponsored by seven leading firms from distinct industries, including aerospace, energy, and financial services. "The research is really informed by problems that industry is facing—and then it makes its way back out of the laboratory to address the problems," says Lori Glover, managing director, CSAIL Alliances, and executive director, Cybersecurity@CSAIL.

(IC)³ includes 23 member firms across sectors, with multiple representatives from each industry. In general, companies choose a specific "stool" to affiliate with, but find a number of opportunities to cross-pollinate as CSAIL sponsors may attend (IC)³ meetings, and (IC)³ partners may attend CSAIL meetings. This overlapping cooperation also occurs in many other ways. The two centers have jointly organized events, such as a panel on cyberinsurance and a detailed presentation of the Ukrainian power grid attack.

Part of that effort involves collecting data from companies to compare spending trends with breaches at different organizations. At the same time, Grochow and others, including Madnick and principal research scientist Michael Siegel, are proposing to use MIT as a laboratory to test the effectiveness of one generally accepted security practice: two-factor authentication, in which users must present a combination of evidence such as a password and a code texted to their smartphone to gain access. Two-factor authentication was recently mandated on campus, and Grochow is hoping to collect data that would one day allow a security professional to predict the percentage drop in data breaches as a result of implementing it. Overall, "the point is to quantify how effective some of these common practices are and balance that against the cost," he says.

THE PRICE OF HUMAN NATURE

Incorporated in these calculations, however, is a growing effort to understand how the so-called "human factor" can undercut pricey defense systems. In recent years, it's become clear that no matter how good firewalls and virus protection software may be, people often make mistakes that allow cyberattackers easy entrance. For example, phishing schemes—in which attackers send emails posing as someone well known to the recipient—have been highly successful in convincing people to give up passwords, bank account information, and other sensitive data with almost no coercion. One recent example—the May 2017 "WannaCry" attack—impacted over 200,000 computers in thousands of corporations in over 100 countries within hours.

In other situations, human efforts to cope with the complexity of security measures makes them more vulnerable to attack. Catherine Tucker, Sloan Distinguished Professor of Management and professor of marketing, found that the number of publicized data breaches actually increased after organizations implemented encryption technology, based on a study of hospitals published in 2011. Other studies have shown that mandating frequent password changes can be counterproductive. The reason? Faced with hard-to-remember passwords, employees often resort to shortcuts that make it easier for thieves to enter, such as writing passwords on sticky notes, Tucker and co-author Amalia Miller of the University of Virginia hypothesized. Pew research backs this up: 49 percent of respondents admitted to writing down passwords to help remember them.

The upside of human error issues is that they don't always require high-priced tools to fix. "There are a lot of small behavioral things organizations can do that help a lot," says Grochow. For his part, he asked all of his employees to add a line to their email signature saying "No one in our department will ever ask you for your password" when he headed information systems and technology for MIT. "That meant that hundreds of people saw that message multiple times every day—an easy and effective way to get the point across and affect behavior," he adds.

CYBERINSURANCE

MIT has been asked by the Geneva Association, the major insurance think tank, to explore the opportunities and challenges of cyberinsurance. Madnick is working with the Boston Consulting Group, and researchers, such as Howard Shrobe in CSAIL, on technologies to reduce risks. Choucri is studying government regulations and how they may even be in conflict for multi-national operations, and other colleagues at MIT Sloan are examining better ways to measure risk, especially for rare potential catastrophes.

A TIPPING POINT

Will cybersecurity still be an issue that keeps executives up at night 10 years from now? Most likely, yes. "The good guys are getting better, but the bad guys are getting badder faster," says Madnick. But armed with better data, smarter networks, and a more holistic view of how to protect themselves, executives may be able to get back to sleep faster. ● ● ●