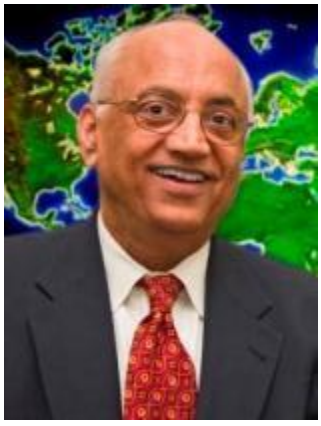
CyberPro
Keeping Cyberspace Professionals Informed
Volume 7, Edition 12
June 12, 2014

SENIOR LEADER PERSPECTIVE: VENKATESH "VENKY" NARAYANAMURTI BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, HARVARD UNIVERSITY



Venky" Narayanamurti is the Director of the Science, Technology, and Public Policy Program at the Belfer Center for Science and International Affairs at Harvard Kennedy School (HKS). He is also the Benjamin Peirce Professor of Technology and Public Policy and a Professor of Physics at Harvard. He received his Ph.D. in Physics from Cornell University in 1965. He also has an Honorary Doctorate from Tohoku University. He spent much of his scientific career at Bell Laboratories where he became Director of Solid State Electronics Research in 1981. From 1987–1992, he served as Vice President for Research at Sandia National Laboratories in Albuquerque, New Mexico. At Sandia, he oversaw a research portfolio of $250 million which spanned its missions in defense, energy, environment, and economic competitiveness. From 1992–1998, he served as Richard Auhll Professor and Dean of Engineering at the University of California at Santa Barbara (UCSB). During his tenure there, the number of faculty elected to the National Academy of Engineering (NAE) in the UCSB College of Engineering grew from three to nineteen. In 2005, through the generosity of an anonymous donor, an endowed chair in his name was established at UCSB. From 1998–2008, he served as Dean of the Division and then School of Engineering and Applied Sciences at Harvard University. At Harvard, he saw the renewal of Engineering and Applied Sciences through a greatly enlarged faculty and the creation in 2007 of the first new school in seventy years. During his tenure as Dean, twenty-two endowed chairs were raised, research funds doubled to approximately $40m, and new linkages with industry were established. During 2003–2006, he was concurrently Dean of Physical Sciences at Harvard. Several enhancements to the physical infrastructure including a new 90,000 squarefoot Laboratory for Interface Science and Engineering were undertaken. Narayanamurti has published widely in the areas of low temperature physics, superconductivity, semiconductor physics, electronics, and photonics. He is the author or co-author of more than two hundred peer-reviewed scientific publications.

NSCI: Can you tell us about a few of the cybersecurity-related initiatives, planned or underway, at the John F. Kennedy School of Government?

Narayanamurti: The Belfer Center for Science and International Affairs at Harvard University has long had a tradition of research on security. It's one of the most preeminent programs in the world and has long focused on areas such as nuclear proliferation and terrorism. The Center promotes an ongoing initiative called the Cyber Project, which hosts Fellows and fosters research on issues of technology, security, and privacy. These all intersect in interesting ways, and our research must also involve the private sector, because it is integral to the advance of technology worldwide. More generally, all of our

programs at Harvard Kennedy School seek to interface technology with the relevant legal issues and how they affect public policy. While that's the overall thrust, we're concentrating on a few areas. We have very strong programs in energy and electricity policy, and we're looking at how cybersecurity impacts physical infrastructure including energy security and electricity grids. Another area is cybersecurity effort for defense purposes, where economic threats are just as important for defense as ones targeting military installations. The cyber threat to the economy is bigger than any other I can think of. Cyber threats have only been recognized as important over the last few years – it's still an emerging field, but an extremely important one for us to get ahead of. That is an underlying goal of both the Cyber Project and the Executive Education program that grew out of it.

NSCI: I understand the school is about to start a new Executive Education program on Cybersecurity: the Intersection of Policy and Technology. What is the program's intent and content?

Narayanamurti: It is our goal to give leaders around the world the necessary tools to develop a real, actionable understanding of the ever-increasing threats of the cyber world. In an age where cyber attacks are rapidly increasing, threatening critical infrastructure and international security, the need to bring public policy and technology leaders together has never been greater. The new Harvard Kennedy School Executive Education program, "**Cybersecurity: The Intersection of Technology and Policy**" will take place from **July 27-August 1**, and immerse these leaders in a unique and intimate learning environment led by renowned faculty and security experts. Faculty Chairs are Jim Waldo, Chief Technology Officer at Harvard University, and Tad Oelstrom, director of the National Security Program at Harvard Kennedy School. And we'll obviously have people from the policy side including Joe Nye who, in addition to being a senior faculty member and former Dean of Harvard Kennedy School, is one of the leading thinkers in national security more broadly, including the use of soft power and other issues central to technology and security. For this, we will discuss not just the specific threats, but also what a robust cybersecurity policy looks like, from design to implementation and evaluation. We hope participants will leave our program well-equipped to face and defeat today's cyber threats, and that by delivering this important knowledge in key areas, their organizations and regions will become hardened against those threats.

What should participants expect to walk away with?

Narayanamurti: Participants in the executive education program will enhance their ability to identify, evaluate, and respond to current and emerging cyber threats; develop frameworks for the design of both cybersecurity policy and technology, and – perhaps most importantly - leave with a lasting network of new colleagues. They will learn about some of the work in emergency response systems, physical infrastructure, and how to expose vulnerabilities before they cause damage. One of the big areas of concern for both Department of Defense and operations relates to what are known as "Zero-days" or "0-Days." Zero-days are previously unknown and unpublished vulnerabilities; exploits and attacks designed around these flaws are very difficult to stop. Zero-day malware can be impervious to traditional antivirus software and other defensive strategies. Controlling the spread and exploitation of zero-days is a serious challenge for both business and policy leaders. Our research fellows have created case studies on zero-days which help illuminate the complex policy challenges. Part of the Executive Education program will cover those case studies, as well as working in groups on table-top exercises that will give participants experience on how to actually address cyber threats.

How does someone apply?

Narayanamurti: We are now accepting applications for "**Cybersecurity: The Intersection of Policy and Technology**," which is running at Harvard Kennedy School from July 27-August 1. The course is designed for a broad range of policy actors and technology experts from around the world who play strategic decision-making roles in both public and private organizations. To learn more about the curriculum and submit your application online, please visit the program website. The deadline to apply is June 27.

NSCI: How would you say the U.S. is doing in collaborating with other countries to improve our national cybersecurity? What improvements would you like to see?

Narayanamurti: The national arena is extremely important. The Internet is a global phenomenon, and one of the things we at the Kennedy School are doing with our colleagues at MIT is to hold a series of workshops establishing norms – basically developing certain standards that could be agreed upon and starting to get a sense of what response systems might look like. The U.S. has very close ties with our European partners, but on some of these issues we'll eventually have to work with China, Russia, and India; all of whom are major players in the IT space. It's still an evolving area. But I think it's important to agree on certain norms and standards – rules of the game – to operate by. Of course people might flout the rules, but at least we need to begin a rational discourse. The role of the university, and the Belfer Center specifically, needs to be in that first phase – to foresee and provide opportunities for dialogue and among leaders.

Many of the threats in cyberspace may be nongovernmental; we don't have to assume that all attacks come from states. Individuals and small groups of hackers may have an inordinate influence without being connected to a state – an important difference from nuclear proliferation threats.

NSCI: There was a recent report, with recommendations, on decentralizing cyber command and control. What's your view?

Narayanamurti: I've read only a brief part of it, but clearly this could be an important issue. The way the Internet was designed by computer scientists and electrical engineers back in the 70s and 80s was as a distributed, open network. That is both its strength and its weakness. It's like democracy in that respect – its openness is both its strength and its weakness. I actually believe you cannot have a purely centralized structure because the very nature of the Internet is that it is dispersed. Perhaps we must develop a kind of hybrid, with both command-and-control mechanisms at the central level, and the appropriate interfacing at the distributive level. This will be an important area of study for policymakers for years to come.

NSCI: While all organizations need to work together when it comes to cybersecurity, the motivations, areas of expertise, access to information, etc. vary when it comes to cybersecurity. How would you define the "lanes in the road" of industry, academia, government, and military as they relate to cybersecurity?

Narayanamurti: This came up with the unfortunate recent leaks in the NSA, and other breaches of security. Private companies have business motivations that are obviously different from government's concerns; and universities' role must be primarily to have an open discourse. So the stakeholders have dramatically different interests. The Internet was designed for researchers so they could communicate freely and the whole system was designed on the basis of trust. That's why we need to develop rules of the road with other states as well so you can have a firm foundation of trust we can all operate by. The interests of academia industry government are often common – nobody wants thieves, obviously – but balance between protecting information and having open information is complex, and ultimately if the trust is broken, that's a very serious issue. We have to balance that with the need for communication against the need for privacy and security. If there is data that must be kept secure, you'll have to isolate that because you can't really operate in the open market where people will find a way to break the code.

NSCI: What are a few key improvements you would like to see to our national cybersecurity policy and strategy?

Narayanamurti: Having increased security is going to be important for lots of things other than just espionage. I'm talking about robbery for economic gain. That I see as a bigger threat than almost anything else. But when you have too tight security, you can't do your work, so through emerging technology, we'll have to keep balancing risk with cost. If you put too many rules early on, then the innovation can be stifled. There are many computer scientists who believe that the best defense is to have a truly open network because then hackers can make small damages but can't bring the whole system down. This is complex and will be the subject of continual debate. Our job is to make people aware of the risk, help them understand the technology, so then they can decide what's best for their own local cases.

NSCI: There has been a lot of media attention given to protecting our critical infrastructure, specifically the power grid, from cyber attack. What are the key ingredients (e.g. people, process, technology, policy) in getting this done? What is your assessment of how we are doing?

Narayanamurti: I would say it's very much still in its infancy. Obviously, electricity and banking infrastructures are critical. There have been some famous breaches in the banking sector, but in the electricity industry, the public is less aware. We have to determine the possible levels of attack, then say "these are the standards we're going to operate under, and that's what has to happen." We have environmental standards, we have fuel standards, soon we're going to have standards of cyber protection that balance the costs against the risks for critical infrastructure. We currently have federal cybersecurity standards for the bulk electric systems—which is an important step. The standards are improving, but, of course, much work is still left to be done. Thinking about how to develop standards for other critical infrastructures, finding the right mix between security and innovation (as well as other concerns), is an ongoing challenge.

NSCI: How is the "Internet of Things" going to change the way we think about cybersecurity? Is it more than just adding more things to the network, or are there going to be some different challenges / concerns?

When Stuxnet occurred and the centrifuges in Iran were affected, it showed that cyber attacks can cause physical damage. The growth of the "Internet of Things" heightens the attack space—it creates a host of new possible targets. This is an area that needs to be studied carefully because, as we now know, even the physical infrastructure can be disrupted as we use information technology. At the same time, the thing that has to be done right now is not to overregulate, but begin to develop metrics and standards, which we will continually monitor and improve as technology advances. Consider air traffic controllers and airline reservations systems. If these were corrupted, it could cause the system to go down. The economic and human costs could really be quite significant. As the "Internet of Things" becomes a reality, we need to prepare the public, ask the right questions, and make rules that are flexible and not rigid. This is an innovative, evolving technology.

NSCI: Thank you very much for taking the time to visit with us.