Martin E. Hellman

Stanford School of Engineering Hero Lecture

The Wisdom of Foolishness

January 29, 2013

Suggested Reading

YouTube Link

If you haven't heard the talk, it is accessible on YouTube.

Abstract of talk

When I first started working in cryptography in the early 1970's, almost all of my colleagues told me I was crazy because NSA had a huge budget, so how could I hope to discover something they didn't already know? And, I was warned, if I did anything good, they would classify it. Those arguments had validity, but with hindsight, it was very wise to take on that "fool's errand." This talk explores several such "tiltings at windmills" that turned out well. (It would take much longer to list all those that didn't!)

On cryptography

David Kahn's book, *The Codebreakers*, is the classic book on the history of encryption, but was written before public key cryptography was invented. Steven Levy's *Crypto* is a more recent history, which includes both public key and an account of my fight with NSA over the freedom to publish my papers. Both are great reads and written for a general audience – they do not require a mathematical background.

For a simple explanation of how public key cryptography works, including the strong box analogy used in my talk, see Andrew Myers' Stanford News article "Encryption leads Stanford's Martin Hellman into National Inventors Hall of Fame," and skip down to the section "Elegant and complex."

For a more complete, but more mathematical description, see my 1976 paper with Whit Diffie, "New Directions in Cryptography," This paper introduced the concept of public key cryptography and introduced what is often called "Diffie-Hellman Key Exchange." Because it builds on the independent work of Ralph Merkle, I have argued that if names are attached, it should be called Diffie-Hellman-Merkle Key Exchange. For more papers on cryptography, see my list of publications, including links to many in PDF.

Defusing the Nuclear Threat

You can read my current project's home page in about five minutes, but you will be better educated than the vast majority of people on this critical issue. In my talk, I mentioned a statement of support for my approach, which has been signed by a number

of prominent individuals. If you agree, add your name to the petition asking Congress to authorize a study of the nuclear risk. Another good way to keep current is to follow my blog.

My paper "How Risky is Nuclear Optimism?" explains why Quantitative Risk Analysis should be applied to a potential failure of nuclear deterrence. My briefing paper on the 50th anniversary of the Cuban Missile Crisis lists 11 little-known risks from 1962, as well as 11 current-day risks and ways to reduce them. The role of critical thinking in reducing the risk is covered in Handout #3 from my seminar "Nuclear Weapons, Risk, and Hope." The other handouts are also freely available.

Bill Perry's Effort

In my talk, I mentioned how noteworthy it is that two out of seven of this year's class of Stanford Engineering Heroes have devoted their lives to reducing the risk posed by nuclear weapons, the other being former Secretary of Defense, and now Stanford Professor, William Perry. The Nuclear Security Project is Bill's joint effort with Ronald Reagan's Secretary of State George Shultz, Richard Nixon's Secretary of State Henry Kissinger, and former Chairman of the Senate Armed Services Committee Sam Nunn. You can get a free copy of their DVD, *Nuclear Tipping Point*. Note that event these four experienced statesmen have been mislabeled as fools.

Breakthrough: Emerging New Thinking

is the book that I co-edited with Anatoly Gromyko, and that was published simultaneously in Russian and English during the period of rapid change in Soviet-American relations. The book is accessible, free of charge, on line. My Stanford web site has a description of the process that led to it, including why it was "a fool home run." That page also has a copy of Gorbachev's endorsement for the book, and there's a separate page with endorsements from a number other prominent individuals, including a former Director of the CIA.

On saving consumers $1-10 billion in electricity bills and 10-100 Mtons of CO_2

When I bought a new premium brand TV late in 2008, I made sure it was energy efficient in standby mode – which is basically when the TV is OFF, but still plugged in. Ads claimed it used less than a tenth of a watt in standby, but when I checked with a power meter, I found it used an average of 15 watts, 150 times more than advertised. With the high rates I was paying as a result of Enron's "screwing California grandmas," this worked out to over $3 a month, about what a subscription to TV Guide would have cost! For a description of the problem and how Katharine Kaplan at the EPA and I solved it see Energy Star or Black Hole, HDTV's DAM pops Energy Star's Bubble, and EPA Moves to Plug Major Energy Star Leak.

My estimate of saving consumers $1-10 billion is derived as follows:

In 2008, when I bought my TV, worldwide sales were over 200 million units. In 2013, sales of 250 million are projected. Without the new Energy Star requirements, I estimate that at least 10 million TV sets produced per year would have drawn 10 watts more than they do as a result of the new requirements.[1] That results in 100 million watts for each year the new Energy Star requirements would have been delayed had I not contacted the EPA when I did.

> If I had not contacted the EPA, it would have delayed the new Energy Star requirements by at least a year.[2] That results in 100 million watts being saved.
>
> Affected TV's have a 10 year life time. There are 87,600 hours in 10 years, which I rounded to 100,000 hours due to the approximate nature of this estimate. That results in 10 billion kilowatt-hours saved.
>
> The average cost of electricity in the US is $0.12 per kWh, but I rounded that to $0.10 for the same reason as above, so saving 10 billion kilowatt-hours saves $1 billion.
>
> The above estimate was based on a conservative estimate that only 4-5% of worldwide TV sales were affected. (I suspect that the EPA requirements are similar to those of other nations.) The number of affected TVs could easily be 3-10 times larger than assumed above, and the period before the problem would have been fixed if I had not brought it to the EPA's attention could easily be a factor of 2-3 larger than assumed above. Together, a factor of 10 increase over the conservative estimate seems not unreasonable.
>
> The EPA estimates that each kWh of electricity puts 0.00071 metric tons of CO_2 into the air, which I rounded to 0.001. So 10-100 billion kWh equates to 10-100 million metric tons of CO_2 saved. A metric ton equals 1.1 of our tons, a negligible difference within the accuracy possible here.

---

[1] The 10 watt savings comes from the new EPA rules vs. the 15 watts my set was using. The 10 million sets per year was estimated as follows: I participated in two teleconference calls hosted by the EPA with TV manufacturers, and most of the participants strongly objected to my proposed change, indicating that the problem was not unique to the brand I had purchased. Even if the problem affected only that brand, their annual TV sales average around 20 million units. I suspect that the EPA EnergyStar requirements are similar to those of other nations, implying global impact, but US TV sales are a significant fraction of global demand.

[2] In addition to the question of how long it would have taken someone else to notice the problem and whether they would have been "foolish" enough to ask the EPA to change their rules, I contacted the EPA at a propitious time because Ms. Kaplan was in the process of formulating the next generation Energy Star requirements for televisions. Those standards are changed only about once every two years.

Other notable examples of the wisdom of foolishness

In my talk I used the following four examples, from emails sent to me by the "wise fools" involved, slightly edited. There are many others.

Vint Cerf, pioneered the Internet (and another Stanford Engineering Hero): "Packet switching was regarded as crazy, even after the great example of the ARPANET. Most conventional communications engineers thought it would not handle speech let alone video. Of course, it got better and better over time. The naysayers believed that store and forward would have too high a latency to be useful. They were wrong." [Today, DSL speeds are over 100X greater than even John's early projection, and DSL has 70% of the worldwide broadband market.]

John Cioffi, the father of DSL: "In 1979, as a young kid fresh out of Stanford, I got laughed out of the room in my first DSL meeting at Bell Labs when I pushed for more speed than the 160 kbps then coming into discussion. I said 1.5 Mbps should be possible on the existing twisted pairs."

Federico Faggin, the designer of the first microprocessor, and **Ted Hoff**, its architect: "In 1970 when I was designing the world's first microprocessor, the CEO of American Micro Systems, then the largest producer of random-logic custom ICs [a technology which lost market share to microprocessors] was quoted in Electronics News as saying something like, 'Whoever thinks that a CPU (the word microprocessor had not yet been coined) will replace random logic is out of his mind.' I remember cutting out that article and posting it in my office as an added incentive to prove such myopic observation wrong!"

Brad Parkinson: chief architect of GPS (and another Stanford Engineering Hero): "The Air Force thought GPS was foolish. They saw no value in precision weapons delivery and certainly did not identify with the Civilian Applications (which I told congress from the start was a part of the system). They also thought that the user equipment would be prohibitive, but we could foresee the digital revolution underway. The first GPS units weighed about 150#, used about 2Kw and cost about $250K. Today a GPS receiver fits on a chip weighing a fraction of an ounce, uses milliwatts of power, and costs (chip only) about $2. None are so blind as they who refuse to see. The Air Force generally persisted in their view, until the first Gulf War showed what the system could do.