THE 5 BIGGEST CYBERSECURITY MYTHS, DEBUNKED

- PETER W. SINGER AND ALLAN FRIEDMAN

"A DOMAIN FOR the nerds." That is how the Internet used to be viewed back in the early 1990s, until all the rest of us began to use and depend on it. But this quote is from a White House official earlier this year describing how cybersecurity is too often viewed today. And therein lies the problem, and the needed solution.

Each of us, in whatever role we play in life, makes decisions about cybersecurity that will shape the future well beyond the world of computers. But by looking at this issue as only for the IT Crowd, we too often do so without the proper tools. Basic terms and essential concepts that define what is possible and proper are being missed, or even worse, distorted. Some threats are overblown and overreacted to, while others are ignored.

Perhaps the biggest problem is that while the Internet has given us the ability to run down the answer to almost any question, cybersecurity is a realm where past myth and future hype often weave together, obscuring what actually has happened and where we really are now. If we ever want to get anything effective done in securing the online world, we have to demystify it first.

Myth #1:Cybersecurity Is Unlike Any Challenge We Have Faced

It's easy to feel overwhelmed by the faster-than-light pace of global information networks. Yet nothing is ever truly new: imagine how the Victorians felt as communications and commerce went from horse and wind powered to wired telegraphs and then wireless radio and they had to wrestle with how to regulate it all.

Having a sense of history can guide our responses to the novelties of our own era. This is not just about learning from Internet history and how we got here, but also learning from fields beyond IT. For instance, in pondering the proper role of government, we can look to the examples of the most successful agencies in history, such as the Centers for Diseases Control, and what public health can teach us about the value of prevention, the merits of awareness and education, and trustworthy mechanisms of sharing information. Or if wrestling with the threat of criminal and quasi-state-linked groups in a global commons, look to the age of sail and how the original pirates and privateers (who China's hacker collectives share much in common with) were chased from the seas through a mix of action against their marketplaces and the creation of international norms. If

thinking about the problem of private actors and their externalities for a shared commons, we might turn to the legal and economic tools used to fight environmental pollution.

There are no perfect fits, no turnkey solutions, but many of the issues we face are not completely new.

Myth #2: Every Day We Face "Millions of Cyber Attacks"

This is what General Keith Alexander, the recently retired chief of US military and intelligence cyber operations, testified to Congress in 2010. Interestingly enough, leaders from China have made similar claims after their own hackers were indicted, pointing the finger back at the US. These numbers are both true and utterly useless.

Counting individual attack probes or unique forms of malware is like counting bacteria—you get big numbers very quickly, but all you really care about is the impact and the source. Even more so, these numbers conflate and confuse the range of threats we face, from scans and probes caught by elementary defenses before they could do any harm, to attempts at everything from pranks to political protests to economic and security related espionage (but notably no "Cyber Pearl Harbors," which have been mentioned in government speeches and mass media a half million times). It's a lot like combining everything from kids with firecrackers to protesters with smoke bombs to criminals with shotguns, spies with pistols, terrorists with grenades, and militaries with missiles in the same counting, all because they involve the same technology of gunpowder.

Good strategy is not about press-release numbers and lumping together unlike things for shock value–much as in the real world, we need to disambiguate online threats, weigh the risks and prioritize how and who should address them.

Myth #3 This Is a Technology Problem

In the tech support world, there's an old joke about "PEBCAK," or Problem Exists Between the Chair and Keyboard. Cybersecurity really is all about people and incentives. There are plenty of important technical fixes and new tools to adopt, but if organizations and individuals aren't willing to invest in securing themselves, then they will remain insecure.

The most important thing we can do is a mentality shift from fear and ignorance (which leads us to be taken in by silver bullet solutions and false hopes for some man on cyber horseback

to rescue us) to working toward what matters more: resilience. Defense and deterrence are good, but as long as we use the Internet, we will always have risk in our cyber lives–from criminals, from enemies, and from plain old-fashioned bad luck. The key is how you can power through them and bounce back quickly from any setbacks. "Keep calm and carry on" should be the mantra, both for the systems we use, but also for our psyches. This especially applies to leaders and media stoking fears by constantly citing scenarios such as the power grid going down or Wall Street being knocked off line. Squirrels cause hundreds of power outages each year and have shut down trading on NASDAQ twice. If we can survive the real world versions of Rocky and Bullwinkle, we can also become more resilient against the feared but still fictionalized dangers on the cyber side.

Myth #4: The Best (Cyber) Defense Is a Good (Cyber) Offense

Senior Pentagon leaders talk about how a couple of teenagers sipping Red Bull in their parents' basement could carry out a WMD style attack, and indeed, one report stated that the offense would dominate "for the foreseeable future." This, in turn, has driven the Pentagon to spend roughly 2.5 times more money on offensive cyber research in its yearly budget than it has on defensive cyber research.

The reality is more complex. The famed Stuxnet, a digital weapon that sabotaged the Iranian nuclear program, showed the dangers of new generations of cyber threats, but also illustrated how they require expertise and resources beyond just sugary drinks. Red Bull gives you wings, but not the instant expertise to attack at an advanced level. Stuxnet's creation required everything from intelligence analysis and collection to advanced knowledge of engineering and nuclear physics.

More important is that it's not the right strategy. This is not the Cold War of some binary relationship, where you just have to deter one other state with similar capabilities and stakes in the game. When there are countless and diverse attackers out there, spending far more on offensive breakthroughs as our primary answer is a lot like thinking that the best way to protect your glass house from tornadoes or the neighborhood kids or a terrorist is to buy a rock sharpening kit. It may not be as sexy, but in both Superbowls and cybersecurity, the best defense actually is a good defense.

Myth #5: “Hackers” Are the Biggest Threat to the Internet Today

There are bad guys out there on the Internet, doing and planning bad things. But if we don’t watch out, the cure can end up worse than the disease. The Internet depends on an ecosystem of trust and we are seeing it threatened in all sorts of ways. This is where the cyber crime against Target meets NSA metadata collection meets the Chinese Great Internet Firewall and the 82,000 blacklisted websites in Russia. They all work against the confidence in, the openness of, and collectively shared governance of the Internet as we know and love it.

In response to online threats, many governments around the world have increased their calls for greater controls and “reforms” of Internet governance, seeking to crack down on free expression and civil society in the name of domestic order, and to throw up technical trade barriers in the guise of national security. We must be very wary of any proposal to protect us from online dangers that that ends up destroying the most powerful tool for political, economic, and social change in our lifetimes, if not all of history.

HYPERLINK "http://www.wired.com/2014/07/debunking-5-major-cyber-security-