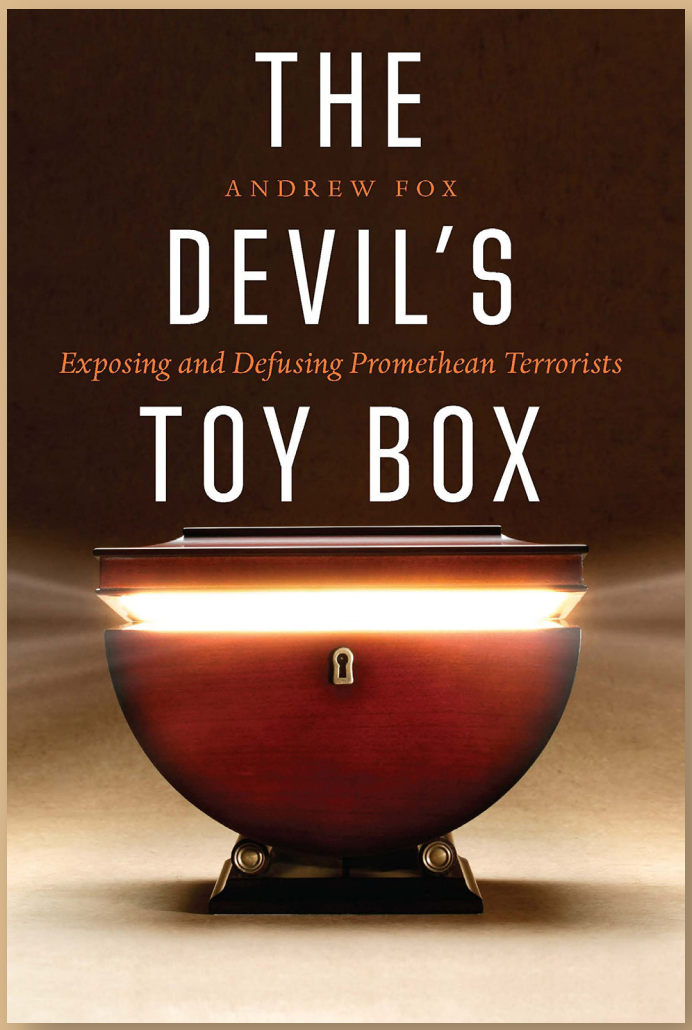

Ted Lewis Reviews Andrew Fox's *The Devil's Toy Box*

By Ted G. Lewis

Suggested Citation

Lewis, Ted. Review of The Devil's Toybox by Andrew Fox. *Homeland Security Affairs* 18, Article 14. www.hsaj.org/articles21677

"Stop here, so I can collect the mail," I said to my wife as our car approached the bottom of our steep driveway. I wanted to avoid the hike up-and-down the long road that separated our house from our country mailbox. Even though it was a sunny day perfect for walking, I always tried to avoid it like COVID-19.

Inside the extra-large mailbox was a large heavy package. "Is it an IED," teased my wife? It could be, but no, it was Andrew Fox's new book, *The Devil's Toy Box*. I carefully unwrapped the FedEx package only to find another wrapper, which resisted my attempts to rip it open. "It must be important," I said to nobody in particular. I gave up trying to rip the package open and resorted to scissors. "Ah, at last," I nearly screamed! With the book in tow, I immediately began to read, jotting down notes as I progressed through each chapter – some of which were tough to read because of the gruesome scenarios presented by Fox.

Do you see what I just did? I used the first two paragraphs to illustrate my laziness and eagerness to read Fox's book without explicitly saying so. Why didn't I just say that I am lazy and eager to read the book? Telling stories is touted as a better way to educate people in the current age of video and short attention spans. For example, Pythagoras of Samos (the triangle guy) contributed much to ancient mathematics, but he was much more interesting as a cult leader and badass. His story helps to make the mathematical medicine go down, so I often use it to motivate students. This is the current fashion in education – the *narrative form*.

The narrative form is how Fox tells his readers about the lessons learned while he attended the homeland defense and security master's degree program at NPS/CHDS (Naval Postgraduate School/Center for Homeland Defense and Security). Sometimes using real exploits with real people and other times using made-up scenarios, Fox brings the reader inside the heads of the bad guys. Over half of the book is synthetic – made-up stories used to teach by allegory. It can be disturbing because it is so real.

Take the counter-terrorism course for example: it is better to get inside a terrorist's head via a scenario – a story – than listening to a lecture about the different kinds of terrorists and their goals. Fox illustrates the different kinds – jihadists, eco-terrorists, white supremacists, hackers, etc. – by telling a real or imagined story. For example, he makes up one scenario about 3D printing to make a gun that is then used to kill people, and another about CRISPR technology used to build hallucinatory drugs that could be used to foster mass hysteria at Disneyworld. It is his *Westworld* TV drama put to good use.

Fox dives into the mental states of the terrorists who bring calamity down on unsuspecting people, so the reader gets a visceral feeling in addition to the facts. It is a mechanism that works well in homeland security because there are plenty examples in real life as well as opportunity for imagining what might happen. And this is his ultimate goal – to get the student-reader to think out of the Devil's box and prevent or avoid the known unknowns.

His stories can get bloody and horrific as they should, because it is real life. I especially enjoyed reading about the black hat who hacked into a patient's computer controlled prosthetic because I wear a pacemaker. Pacemakers are notoriously easy to hack into. The criminal can simply command it to stop pacing or run wild, pumping too much blood until you die . In another semi-realistic episode, he dramatizes the take-over of a truck, by a hacker intending to do harm. Once under the control of a malicious hacker, cars and trucks can be used as weapons.

It is much more interesting to read a dramatization than simply stating the facts. Of course, none of these exploits actually happen – or do they? Moreover, will they happen in the future? That is the question.

Homeland security is obsessed with finding the answer. On the one hand, there is ample opportunity for terrorist attacks in target-rich America. On the other hand, there is limited funding for response and prevention. In addition, the politics of security is at best unsettling. Let me be blunt: In the USA we go for long periods of time ignoring the threats around us, followed by hysterical over-reaction following a major incident. Take the hubris fallout of the 9/11-Afghanistan conflict and more recently the COVID-19 pandemic as the most recent example. After years of ignoring warnings by elites like Bill Gates and the CDC, we plunged into the pandemic with something like $1.6 - $4.0 *trillion* in stimulus response. We suffer from schizophrenia, among other things.

In an ideal world, we might use technology to predict catastrophes. Alright, prediction isn't possible, but forecasting is. Can we forecast the array of possible future attacks, prepare for a handful of the most likely, and keep a little aside for prevention? This is the problem addressed in a colorful way by Andrew Fox.

Fox examines Promethean technologies defined as technologies that give attackers God-like powers, or at least power on par with the military and omniscient governments. He considers CRISPR, 3D printing, and hacking into power grids Promethean. I am not so sure they matter all that much. The terrorist attacks of 9/11 used a box cutter and airliner; most jihadists use simple homemade explosive devices – IEDs. The slaughter of school children (and people in general) is the result of cowardly use of simple firearms. Internet exploits have done serious financial harm, but only a handful of human casualties have been reported. Never mind this, right now. Read on!

Eventually, Fox boils everything down to risk and risk analysis in an attempt to separate out the emotion of politics, the limitation of funding and time, and the overwhelming number of options available to terrorists. This is about the human side of homeland security, not the climate change side or the critical infrastructure side. After all, the human side is complicated enough.

So, what is the risk? In chapter 4 Fox takes on the challenge of risk analysis. Risk analysis is an essential tool in the practitioner's toolbox, but it is perhaps the most misunderstood technique in homeland security. Risk, defined as "expected loss" or "probable loss," is always a difficult climb for homeland security professionals, because it is so analytical. Homeland security practitioners are notoriously adverse to numbers and quantitative logic. So, Fox illustrates risk assessment using scenarios, much like the U.S. Coast Guard does with Maritime Security Risk Analysis Model (MSRAM). MSRAM is a formal model that combines numbers with scenarios like drug smugglers using submarines or ports being blocked by sunken ships. You get the idea.

I'm not sure Fox's narrative approach works in the real-world, but for the number of quantitatively challenged student-practitioners it probably does. However, narratives like the one presented by Fox emphasize consequence and ignore likelihood. In this regard chapter 4 is really about threat assessment more than risk assessment. To see the difference, consider the consequence of another 9/11 event. It is huge, but the likelihood of it happening again is near zero. Black swans are big consequence events, but they rarely happen. So, what is the risk of some madman taking down the Golden Gate Bridge? The consequences are enormous, but the likelihood is so small that homeland security spends relatively little on preventing bridge attacks.

The inadequacy of chapter 4 is remedied somewhat by chapter 8 on Promethean Spyglass – the method of full-blown risk assessment proposed by Fox. It reverses course and recommends a mathematical approach using scenarios, probabilities and everything. This suggests that chapter 4 is an unnecessary diversion because Fox replaces it with a more rigorous quantitative method in chapter 8. What happened to the stories? They are converted into scenarios that drive the risk analysis. The Spyglass method combines scenarios with probabilistic risk analysis (PRA) more in line with what is actually practiced. In its simplest form PRA says risk is probability of an exploit multiplied by its consequence. So, for example, if the likelihood of a cyberattack is estimated to be 50% and its consequence (cost) is estimated to be $10 million, then expected loss is 0.50 x $10 million or $5 million: simple arithmetic.

Even then, PRA has detractors. The first objection is that ranking PRA results to decide where to put resources is problematic and often wrong. To illustrate, compare the PRA risk of a cyberattack with consequence $100 million but likelihood of 5%. PRA risk here is also $5 million – exactly the same as the risk above. So, how does one rank them? In addition, PRA does not account for what Eric Saylors defines as "quantifying the negatives", e.g., adding up the cost of something NOT happening. For example, in California – the land of forest fires – how do we quantify the lives saved and property protected by extinguishing fires and registering the (reduced) damages compared with (greater) damages if the fire burns itself out? Firefighters are evaluated on the consequences of victories over fire, not on the consequences of damages compared with failures. Risk analysis is much more complicated than Fox says.

The Devil's Toy Box contains a lengthy chapter surveying science fiction and science fiction writers. The purpose, of course, is to convince the reader that sci-fi authors possess some magical ability to imagine superior scenarios. Unlike the rest of us, sci-fi writers can conjure up fantastic exploits and predict future technologies unimaginable to mere mortals. Fox illustrates this by listing Asimov and his imagined earth-orbiting satellites circa 1940, and Jules Vern's electric submarine circa 1870. He doesn't mention sci-fi missing the rise of the Bomb in the 1940s or the World Wide Web in the 1980s. (William Gibson's 1984 novel Neuromancer implied some sort of network, but even Gibson failed to imagine the Web of today. In 1984 the ARPANet, a.k.a. Internet, was nearly 15 years old).

Fox is obviously impressed by the professors at NPS/CHDS, where much of the core ideas originated. When I was the Executive Director of CHDS, we talked about recruiting science fiction writers to come up with scenarios. This idea probably began at NPS and the U.S. military, which has long been involved in war games. DoD has been concerned with surprise attacks ever since Pearl Harbor. So, this fits right in.

John Hiles, a research professor at NPS in the late 1990s, invented software that automatically generates stories that are incorporated into virtual reality environments. It is in the DNA of NPS. Fox brings this to homeland security in the form of a well-written book. Moreover, he is able to get inside the characters' heads so we can see what makes them tick. It isn't a pretty picture.

Content-wise the book covers the standard fare of scary exploits: synthetic biology and CRISPR tools, 3D printing, EMP (electro-magnetic pulse) machines, and various forms of cyber hacking exploits. All are asymmetric, meaning they are cheap and easy to acquire, but difficult and expensive to defend against. Fox emphasizes the current impact of asymmetry – emergent behavior. This is the idea that out of combinatorial innovation as explained by W. Brian Arthur, sooner or later one of the combinations emerges and becomes a tool for asymmetric attack. The box cutter used by the 9/11 terrorists is a simple example. More complicated examples come from technical innovation such as the CRISPR, cyber un-security, and machine learning. Fox subscribes to NPS/CHDS professor Rodrigo Nieto-Gomez's notion of, "permanent disruption of high-tech society through deviant innovation."

Chapter 5 dives into a review of forecasting methods – Delphi, Futurism, Scenario Analysis, Red Teaming, Wisdom of the Crowd, and Superforecasting. I won't go into the details of each because it would take too many paragraphs. Instead, I'll relate my experience with forecasting while I was CEO of DaimlerChrysler R&D North America in 1999. After Daimler merged with Chrysler, the bosses in Stuttgart wanted to know wat the future of mobility might be. So, we collected a small group of futurists such as Peter Schwartz, founder of Global Business Network, a corporate strategy firm specializing in future-think and scenario planning, and Stewart Brand of Whole Earth fame and asked them to tell us what the automobile would look like in 10-20 years. The only thing they got right was that somehow the Internet would find its way into the car. They completely missed electric cars, GPS guidance, and self-driving technology. So, it is understandable that I am skeptical of scenario discovery and planning.

Homeland security professionals now realize that protecting everything is too expensive even if it ranks high on a PRA scale. Instead, the strategy is to spend some resources on responding to high-probability, low-consequence events and remaining resources on preventing low-probability, high-consequence events. This isn't perfect, but it settles the conundrum of prevention versus response. If you think about it, we already do this to some extent. Homeland security aims to respond in a timely manner to forest fires, hurricanes, and floods, while it aims to prevent another 9/11 or COVID-19.

The book ends on a scary note. The story Fox tells in chapter 6 is frightening in its approximation of reality. He dramatizes an imaginary attack on the U.S. Secretary of Defense during a hypothetical war between Albania and Macedonia. Fake news is used to convince the public that the Secretary of Defense is a pedophile, and it works! Fake news is used to undermine the credibility of the U.S. government and harm the U.S. attempts to help Albania. Does this scenario remind the reader of current events?

I recommend this book for the lay reader who wants to see what it is like to be a terrorist and how homeland security practitioners approach the terrorist problem. It makes entertaining reading for the non-expert, non-homeland security practitioner as well. I can't wait for the movie.

About the Author

Ted G. Lewis is a retired professor of computer science and former executive director of the Center for Homeland Defense and Security at the Naval Postgraduate School. He spent forty years in academic, industrial, and advisory capacities, ranging from academic appointments at the University of Missouri-Rolla, University of Louisiana, and Oregon State University, to senior vice president of Eastman Kodak Company, to CEO and president of DaimlerChrysler Research and Technology, North America. Dr. Lewis has published over thirty books and 100 research papers. He is the author of Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation (2006, second edition 2014), Network Science: Theory and Applications (2009), Bak's Sand Pile (2011), and Book of Extremes (2014). He received his PhD in computer science from Washington State University. Dr. Lewis may be contacted at tedglewis@icloud.com.

Copyright