Here Be Dragons

Fred B. Schneider
Associate Editor in Chief

This isn't the first time we've been told that the world is flat. In ancient times, ships that set sail for new worlds either returned or didn't: those that returned hadn't sailed far enough, and those that didn't must have sailed over the edge and fallen off, where, as popular belief held, dragons awaited them. As further support for the flat-Earth hypothesis, anyone who ever cared to experiment either saw an obstruction in the distance or a never-ending flat expanse no matter which direction they looked. What else could the world be but flat?

The 21st century "flat world" craze, like its predecessor, also involves India and China, but it's now the transportation of bits and not atoms that hold promise of riches. Communications networks enable the outsourcing of any task that can be conveyed and discharged by transmitting bits. For example, telephone conversations, medical images such as x-rays, and software artifacts can all be encoded using bits. Therefore, telephone customer-help centers, x-ray analysis, and software construction become candidates for outsourcing, effectively exporting jobs from one country to another and reducing costs if the new workforce is less expensive but equally expert.

Today's "flat world" is actually as spherical as ever—it's just better connected electronically and thus metaphorically lacks obstructions. So what does all this hold for cybersecurity? One consequence is obvious—to the extent that bits from one place aren't obstructed from reaching any other place, attackers have an easier time launching their attacks and attacks spread more easily between machines.

The modern "flat world" comprises sovereign countries, with their separate laws, values, and cultures. Differences in laws means that an illegal act in one country might be legal in another; differences in values and cultures means that those differences in law are unlikely to change. The multiplicity of jurisdictions with different laws, with the attendant uncertainty about which laws apply and how they will be enforced, becomes an obstruction in our "flat world" because bits that leave a jurisdiction you trust for one you don't might be subject to abuses that are costly to prevent or remediate. Uniform civil law, that great leveler for commerce, is absent on the international scale. Business relationships between partners only sometimes substitute.

Finally, most security in the physical world is based on accountability of action. Perpetrators of offensive acts fear being caught, convicted, and punished. It's hard to argue with success, so we might contemplate the use of accountability in cyberspace. However, to do so, today's systems and networks would need to be substantially changed because they currently don't provide trustworthy attribution of action. Even if they did, the existence of multiple jurisdictions becomes problematic. There is the obvious concern: which jurisdiction is responsible for conviction and/or punishment? And there is a less obvious concern: can each jurisdiction be trusted to create and preserve attribution for content traveling though that jurisdiction, even if the attribution is for supporting laws that are inconsistent with the jurisdiction's laws. The recent Google-China controversy is just the tip of that particular iceberg.

So our world isn't all that flat after all—at least, not once you take into account realities that aren't easily reduced to economics, such as malfeasance, cultural differences (and its manifestation in law), or people's comfort with trusting what is local, what is familiar, and what they understand. The 21st century "flat world" is an oversimplification of the real world. We can accept that fact and then turn attention to metaphors that focus on the real issues, such as the need to support accountability. Or, we can strive to make our real world closer to the idealized flat world, such as by working to create international uniform laws, extradition treaties, and so on. But to embrace an inaccurate model and base policy on it—here be the dragons. □

Have a comment on this or other articles in *S&P*? Please contact lead editor Kathy Clark-Fisher at kclark-fisher@computer.org. Visit us at www.computer.org/security/.