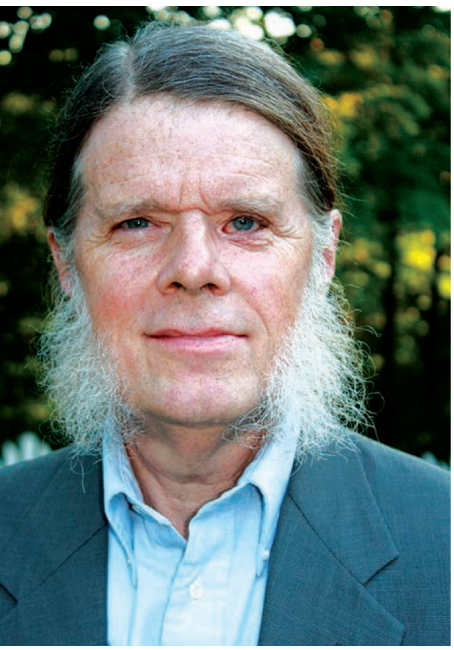

Daniel E. Geer, Jr.
In-Q-Tel

Convergence

Some technologies exhibit positive feedback loops; the effect of their own progress is to accelerate their own further progress, constant acceleration in other words. Using ever more powerful computational models to design ever more powerful computational models is obviously such a case. Obtaining (and holding) a technologic lead in the presence of a positive feedback loop is inherently different than doing so in a field where persistence—just doggedly slogging it out—is the driving mechanism for progress. Put differently, under constant acceleration the distance between two entities can only increase.

A positive feedback loop is a challenging companion ("When you ride the tiger, it is difficult to dismount"). Positive feedback loops are unexcelled for creating change, but they tend to result in undesirable consequences if not moderated by negative feedback loops.

There are areas of R&D a democracy would demur to perfect but an autocracy would not; crafting precision targeting for biologic agents would be a state-level example, just as the major players in surveillance capitalism collect data that no democratic government permits itself to demand or even have. To the autocrat, to the unconstrained entity, some R&D is irresistibly money/power making; it may also be irreversible in the style of opening Pandora's box.

In medicine, a "pathognomonic" symptom is one that is so inherently characteristic of a given disease that simply finding the symptom present confirms the diagnosis. And so I ask, is the presence of a positive feedback loop pathognomonic for the technology in question being dual-use (dual-use in the sense of usable for both offense and defense)?

If the positive-feedback-means-dual-use conjecture is true, then technologies that exhibit positive feedback loops deserve special consideration from a policy perspective because their constant acceleration can only lengthen the lag-time between appearance of a new form of offense and the construction of an adequately responsive defense against it (not to mention the mismatch between a technology continuously accelerating and the step-wise character of policy adoption). What might such technologic areas be?

Synthetic biology is one. Synthetic biology is "the design and construction of new biological parts, devices, and systems, and the redesign of existing, natural biological systems for useful purposes" (https://www.nature.com/subjects/synthetic-biology). Synbio is subject to positive feedback loops—as we learn how specific genes or combinations of genes work, it becomes easier to both direct biology to do things and to learn how more genes operate. This is why having a heterogeneous genomic library with mandated quality, scope, and accessibility (as China is building and the United States is not) and pursuing synbio on a systematic basis (versus university project-by-project or company-by-company) is competitively advantageous. At some point, China will be far enough ahead that the United States can never catch up—that constant acceleration of the positive feedback loop again.

Artificial intelligence (AI) is another (AI culturing new AI), with the added "feature" that without intervention the AI-cultured AI will not be explainable—will not be subject to meaningful interrogation as to why it made such and such a decision. Those who argue for politically/ethically curated training data are essentially acknowledging that same assertion, viz., if you can't ask the AI "Why?" then you can only choose between accepting or rejecting the AI's output. As AIs advance toward crafting other AIs, the level of indirection will make this so if for no other reason (putting aside an AI that learns to lie under interrogation and the ever-present risk that an actual explanation could open up an AI to adversarial games). That effect of constant acceleration yet again. Already the marginal cost of computing, communication, data storage, and AI at the edge are trending toward zero; it will soon be impossible to buy sensors without

Digital Object Identifier 10.1109/MSEC.2021.3106594
Date of current version: 28 October 2021

continued on p. 123

 1540-7993/21©2021IEEE

built-in object recognition or some other form of AI.

With just those examples—the familiar computationally aided design of computation, the synbio contribution to accelerating advances in synbio, and AIs that move beyond self-modification to self-construction—the convergence of any one of those with cybersecurity is worth our consideration.

Why? Because these convergences with cybersecurity seem to this writer to be inevitable. Already it is obvious that the future of humanity and cybersecurity are conjoined; soon it will be the case that, for any one of those possible convergences, the conjoining will be deep, impossible to disentangle, and beyond the reach of trust-but-verify.

Let's imagine a convergence between all of the above, that is to say a computationally growing cybersecurity regime cultured by advances in AI and implemented, at least in part, in synthetic biologic structures. What might we imagine a balance sheet would look like, a balance sheet in terms of pros and cons, advantages and disadvantages, risks and benefits?

Or can we even analyze such a risk-benefit tradeoff space? Take blockchain genomics (the blockchain storage of a person's genome in whole or in part for integrity, anonymous sharing, proof of identity, licensure, etc.) as but one early example of convergence between cyber and other fields showing positive feedback loops. On the one hand, there are the promises/benefits such as fully personalized medical advances heretofore inconceivable. On the other hand, there is the risk of a surveillance that makes Xinjiang facial recognition seem to be small potatoes. What is an adequate response to this convergence? Should liberal democracies make it policy, say, that some things are never put in immutable storage?

The present author is struggling to make even a plausible inventory of what this one example convergence could deliver, and there are many other convergences. But he knows one central thing: ordered liberty depends on putting a speed limit to irrevocable change. ■

Daniel E. Geer, Jr. is a Senior Fellow at In-Q-Tel, USA. His collected works are available at http://geer.tinho.net/pubs. Contact him at dan@geer.org.