Eisenhower Revisited

"If all that Americans want is security, they can go to prison. They'll have enough to eat, a bed, and a roof over their heads. But if an American wants to preserve his dignity and his equality as a human being, he must not bow his neck to any dictatorial government." —Dwight D. Eisenhower, 8 December 1949

Daniel E. Geer Jr.
In-Q-Tel

Eisenhower, Supreme Commander of the Allied Expeditionary Forces in World War II, then university president, and ultimately American president, could parse the consequents of force. He made no move against Franklin D. Roosevelt's "New Deal," but he circumscribed it within a balanced budget. He birthed the containment policy that ultimately defeated Soviet Communism, yet he also initiated the first nuclear test ban. He constructed his unequaled presidential farewell address as a reproof, using a neologism that stuck: the military-industrial complex.

We're about to have something rather more potent. Like some volcanic archipelago rising from the ocean's surface, information security is fast becoming a cyber-industrial complex. The signs are everywhere.

Some of it is laughable, such as a Congressional proposal to "Do Not Track," which, as a matter of logic, can't work without strong authentication, setting the stage for some new bureaucrat to declare, "We had to destroy anonymity in order to save it."

Some of it is brazenly hegemonist, exemplified by nothing so much as the tail that is the entertainment industry wagging the dogs of every self-styled progressive government up to and including seeking the authority to break down digital doors on suspicion alone.

Some of it is Orwellian, such as the various efforts of various nation states to control not what search engines find but what they must then be forbidden to share. How soon do you suppose it is before spidering the Web requires a government license, perhaps one auctioned off the way radio bandwidth is auctioned—for vast sums, yet always subject to seizure should the search engine licensee displease its government licensor?

Some of it toys with addressability itself, as if a predictable, coherent name structure were just another currency. (That one is no prediction, ICANN having now devolved into nothing but a protection racket.)

Some of it reverses the idea of innocence until guilt is proven, which is precisely what the mandated retention of data tries to do—prove a negative, something science has told us can't be done absent perfect knowledge.

Some of it is exactly what the opening quote from Eisenhower invited—a prisoner's comfort—only this time the jailer will be the ISP, deputized against its will to police the cyber health of all users on the ISP's networks, even if those users' machines are better managed after some bot herder pwns them. (The warrant-less wiretap imbroglio proved by demonstration that the bigger the ISP, the less it can resist forcible deputization.)

Some of it is the penumbra of black research budgets, ironically cheered on by a security research community that seems hell-bent on calling every major hack "not all that advanced," probably meaning "I could do it better." (Fifteenth century map makers did the same thing, promising El Dorado if only this or that king would just send in some professionals. Like them.)

But more than any of that, it is a complex, and, as we know, complex systems have notable side effects. The "consumerization" of computing, including such programs as "bring your own computer to work," so obliterates the enterprise data perimeter that the resulting threat can only be countered by instrumented surveillance at the system-call level. The general-purpose computer as a consumer durable is dead; aggregate 2010 Q4 shipments of smartphones proved it. Freedom to tinker? Irrelevant, not to mention near-term nonexistent. What you're buying, which is to say what you (the office worker) are capitalizing for your employer, is an all-singing, all-dancing display device connected to the walled garden of some well-deputized ISP, now with app stores and God-knows-where storage, but no compilers.

As Eisenhower said, dictators always use "security" as an excuse for enlarging their domain,

cont. on p. 87

 1540-7993/11/$26.00 © 2011 IEEE

cont. from p. 88

but in policy documents, unlike in literature, it's the definition of the words that matter more than the sentences that subsequently use them. Sometimes that definition is "security from the great unknown," and other times it's "security from having to choose." Some forces would happily offer the user community a spam-free Internet in return for having complete identity and audit logs of everyone's every action. Those forces are even perfectly happy to have the liability of your risky actions assigned to them, so long as they're permitted to monetize them. If the private sector becomes government's outsourced enforcer of mandated cybersecurity—so that users are never forced to choose between convenience and self-protection—this monetization becomes permanently structural.

We've seen it all before: automobiles are now festooned with cost-ineffective countermeasures for rare, even apocryphal, events. The US Department of Homeland Security threat level is permanently orange, ensuring a robust market for cures that are even worse than their disease. Further food safety regulations mean not safety so much as an escalating barrier to entry for small producers. You think cybersecurity won't soon follow?

Paraphrasing Eisenhower word for word, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the cyber-industrial complex. The potential for the disastrous rise of misplaced power exists and will persist. We must never let the weight of this combination endanger our liberties or democratic processes. We should take nothing for granted. Only an alert and knowledgeable citizenry can compel the proper meshing of the huge cyber and industrial machinery of information security with our methods and goals, so that security and liberty may prosper together. □

Daniel E. Geer Jr. *is CISO for In-Q-Tel and past president of the Usenix Association. Contact him at dan@geer.org.*