# OBAMA'S "ZOO ANIMAL" BROKE FREE AND "CROSSED THE RUBICON"

> At the bottom of it all has been the Bomb. For the first time in our history, the President was given sole and unconstrained authority over all possible uses of the Bomb.
>
> [snip]
>
> Every executive encroachment or abuse was liable to justification from this one supreme power.
>
> If the President has the sole authority to launch nation-destroying weapons, he has license to use every other power at his disposal that might safeguard that supreme necessity. If he says he needs other and lesser powers, how can Congress or the courts discern whether he needs them when they have no supervisory role over the basis of the claim he is making? To challenge his authority anywhere is to threaten the one great authority.
>
> —Garry Wills, Bomb Power

I suppose I'll eventually get around to discussing how the series of condoned leaks portraying President Obama as the Deciderer all rest on the pathetic but true fact that he is only borrowing George Bush's claim to that title.

But for now, I want to focus on the one part of David Sanger's mixed-metahpor saturated installment in the Deciderer 2.0 series that rings most true:

> Mr. Obama, according to participants in

> the many Situation Room meetings on Olympic Games, was acutely aware that with every attack he was pushing the United States into new territory, much as his predecessors had with the first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade. He repeatedly expressed concerns that any American acknowledgment that it was using cyberweapons — even under the most careful and limited circumstances — could enable other countries, terrorists or hackers to justify their own attacks.
>
> "We discussed the irony, more than once," one of his aides said. Another said that the administration was resistant to developing a "grand theory for a weapon whose possibilities they were still discovering." Yet Mr. Obama concluded that when it came to stopping Iran, the United States had no other choice.

With cyberwar, with drones, and (to a lesser extent) with the embrace of the terrorists' transnational methods to fight terrorists, Obama has crossed into uncharted territory of the sort Wills explored in his book, *Bomb Power*. These changes are likely a step beyond the Bomb Power paradigm, whatever that entails.

Yet Obama has only barely begun to think through the ramifications of these tools. He has, instead, focused on the near and overblown threats of Iran and AQAP, not seeing both the strategic implications of even those choices, much less the implications of the sort Wills describes arose in the wake of our use of a nuclear bomb.

The President has embraced waging extralegal war using drones from the Oval Office. The President has embraced using easily manipulable code to wage physical war. What are the implications of these decisions?

Oh sure, Obama started paying attention after the fact. A year ago, he rolled out a "National Strategy for Cyberspace," calling for international cooperation to enforce responsible behavior of the sort we have already violated. Even more recently, DOD has been tinkering with our rules of engagement.

But there are signs it is already too late, the battle lines have been drawn. We've already seen the Executive Branch's refusal to share details with Congress, followed by flaccid attempts to force it to do so.

Sanger's article describes how in 2010 we began to see the unintended consequences of sloppy—or covert—coding.

> In the summer of 2010, shortly after a new variant of the worm had been sent into Natanz, it became clear that the worm, which was never supposed to leave the Natanz machines, had broken free, like a zoo animal that found the keys to the cage. It fell to Mr. Panetta and two other crucial players in Olympic Games — General Cartwright, the vice chairman of the Joint Chiefs of Staff, and Michael J. Morell, the deputy director of the C.I.A. — to break the news to Mr. Obama and Mr. Biden.
>
> An error in the code, they said, had led it to spread to an engineer's computer when it was hooked up to the centrifuges. When the engineer left Natanz and connected the computer to the Internet, the American- and Israeli-made bug failed to recognize that its environment had changed. It began replicating itself all around the world. Suddenly, the code was exposed, though its intent would not be clear, at least to ordinary computer users.
>
> "We think there was a modification done by the Israelis," one of the briefers told the president, "and we don't know

> if we were part of that activity."

Yet Sanger, like any obedient sanctioned journalist, doesn't mention the most ominous unintended potential consequence of StuxNet, one contemplated by the Russians: setting off an explosion at Bushehr. The possibility of setting off—perhaps unintentionally—nuclear explosions without attribution. And we know the Administration is preparing to act even more carelessly in the future. Meanwhile, all our military toys contains hundreds of backdoors, ripe for the picking.

More interesting is how Obama is willingly chipping away at the Bomb Power President, perhaps without noticing. There is, of course, the matter of the Israelis. Can't wage cyberwar with them, can't wage cyberwar without them, so you never know when some surprise code will show up. Heck, we even refuse to admit that they're stealing from us every bit as much as our rivals. Doing so might make us stop and think twice about whether we're prepared to play this game.

I'm most interested in what this entails for secrecy. The Sanger article, of course, is an egregious version of sanctioned leaks of classified information. The most intriguing bit, to me, is this suggestion we've found a way to bridge air gaps.

> In fact, thumb drives turned out to be critical in spreading the first variants of the computer worm; later, more sophisticated methods were developed to deliver the malicious code.

But the most amusing tidbit is this mention of the sabotage we've conducted in the past.

> For years the C.I.A. had introduced faulty parts and designs into Iran's systems — even tinkering with imported power supplies so that they would blow up — but the sabotage had had relatively

> little effect.

The fact that we introduced faulty designs into Iran's systems is, you'll note, precisely the information that Jeff Sterling is currently being prosecuted for, that James Risen is being subpoenaed for. But here it is, dropped into a sanctioned leak story, easily the least interesting nugget.

At this level, then, this story displays the height of the Bomb Power President's abuse of information asymmetry, permitting selected people to spread the same secrets that are criminalized from others.

But the larger tale—particularly the escape of StuxNet and its subsequent exposure—shows the lie of this arrogance. The Chinese, certainly, can take what they want. Bradley Manning allegedly can take what he wants too. And unless the code is perfect, and unless the Israelis refrain from toying with the code, eventually the code, the Bomb Power itself, will become available.

Obama's foolish embrace of these new technologies without considering the larger impact may lead to the decline of the Bomb Power President—of Presidents, generally. It may lead to something far more fearful.

But one thing is clear: he didn't really stop to think about all that before he set free his zoo animal.