Stuxnet's origins decoded: Now we know who did it, but what does it mean?

June 4 2012

David Fidler. Credit: Indiana University

Last week's New York Times adapted a portion of David Sanger's forthcoming "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power," which reveals that the United States has secretly conducted cyberattacks against Iran for several years. Indiana University Center for Applied Cybersecurity Research Fellow and Maurer School of Law Professor David P. Fidler said the article raises important questions. His commentary follows:

David Sanger's article in today's New York Times confirms what many suspected: The U.S. and Israel crafted the Stuxnet computer worm to attack Iran's uranium enrichment program. The operation, code-named "Olympic Games," began under the George W. Bush administration with Israeli participation and was sustained by President Barack Obama. Sanger's reporting solves the attribution question concerning Stuxnet, but his revelations raise troubling issues about the future of cybersecurity, the Internet and cyberspace.

Sanger describes Obama as aware that "Olympic Games" was taking the U.S. (and the rest of the world) into uncharted territory. However, decisions by Bush and Obama subordinated all other considerations to stopping Iran's suspected development of a nuclear weapons capability. Obama kept the attacks going even after the Stuxnet worm escaped and appeared in computer systems around the world -- a willingness to accept continued collateral effects from attacks on Iran.

How the Stuxnet campaign unfolded replicates how great powers have always weaponized new technologies without understanding (or really being able to understand) the implications of such decisions. The Internet proves no different than any previous technology harnessed in the security and military competition among states. The "Rubicon" crossed with Stuxnet is, in truth, a familiar crossing. We know risks wait on the other side, some of which we cannot control.

As Sanger reveals, in light of Stuxnet, some U.S. officials want cyberweapons used more against other threats. The desire for expanded use relates to an aspect of Stuxnet that remains debated: How should use of cyberweapons be categorized in policy and law?

A curious thing about Stuxnet is that commentators often discussed it as "cyberwar," yet few, if any, governments behaved as if the Stuxnet attack constituted an act of war. Sanger's article does not discuss how the

Bush or Obama administration debated or resolved constitutional and international legal questions about using Stuxnet -- was it a covert intelligence action or military operation under U.S. law, or use of force, armed attack or self-defense under international law?

Does resolving the attribution problem change how we think about the Stuxnet attack? This question is important for Stuxnet: Does Iran have the right to use force in self-defense or hold the U.S. and Israel accountable? The question is also relevant to interest in using cyberweapons more extensively. If we expand use, what are we doing in policy and legal terms?

Another risk involves how other countries respond in light of attribution of Stuxnet to the U.S. and Israel. Perhaps attribution will not matter because, before Stuxnet, experts believed that states were seriously exploring espionage and military uses of the Internet. Many perceived Stuxnet as a "game changer" without needing to know who was responsible. If nothing else, identification of Stuxnet's creators will deepen other countries' interests in defensive and offensive cyber capabilities -- a pattern seen many times before with weaponization of new technologies. How far this dynamic goes, and with what consequences for the Internet and cyberspace, remains to be seen, but history tells few encouraging tales concerning this pattern of behavior.

The Obama administration has called for "norms of responsible behavior in cyberspace" and championed global "Internet freedom." Clarity on Stuxnet's origins does not render U.S. support for these ideas hypocritical, but it creates obstacles for achieving them. Other countries will not accept that the U.S. can engage in cyberattacks and cyberespionage without constraint while expecting other governments to behave "responsibly" and ensure "Internet freedom." Sanger's revelations give countries such as China and Russia ammunition in their dogged pursuit of more "international regulation" of the Internet. The

implications of decoding Stuxnet's origins go beyond national security and military concerns to affect broadly -- and potentially profoundly -- the future of the Internet and cyberspace in global affairs.

Provided by Indiana University