ALTERNET

Published on *Alternet* (http://www.alternet.org)

Home > Cyber Arms Control Pipedreams: Why Attempts to Limit Malware Development Are Destined to Fail

Cyber Arms Control Pipedreams: Why Attempts to Limit Malware Development Are Destined to Fail

By Bill Blunden [1] / AlterNet [2]
March 6, 2015

As the extent of the NSA's offensive programs [3] becomes public knowledge, the editorial board at the *New York Times* has recommended [4] that the United States government try to jam the lid back on Pandora's Box by engaging in "international efforts to negotiate limits on the cyberarms race." The editorial board then references Cold War arms-control treaties as a model for future efforts. Yet the history of the Cold War demonstrates that arms-control treaties don't always pan out. Moreover the inherent nature of malware engineering makes the detection of treaty violations nearly impossible.

For example, in 1972 the Nixon administration participated in an international treaty with the United Kingdom and the Soviet Union to ban the production of bioweapons. Unfortunately, the Soviets interpreted the 1972 Biological Weapons Convention as a go-ahead to aggressively pursue an initiative that eventually scaled up into hundreds of tons. According to Kanatjan Alibekov [5], the first deputy director of the Biopreparat, Soviet researchers were up to their necks in biological WMD:

> "In the '70s and beginning of '80s the Soviet Union started developing new biological weapons—Marburg infection biological weapon, Ebola infection biological weapon, Machupo infection, [or] Bolivian hemorrhagic biological weapon, and some others."

Seven years after treaty's ratification approximately 100 people died under suspicious circumstances in the Russian city of Sverdlovsk [6]. The Soviets initially claimed that the deaths were caused by tainted meat. Over a decade later President Boris Yeltsin admitted that the deaths were a result of a clandestine military operation.

Keep in mind that manufacturing bioweapons on an industrial scale required the Soviets to build dozens of facilities and employ thousands of people. An undertaking that wasn't easy to conceal, especially with CIA specialists conducting exhaustive "all source analysis” to ferret out treaty violations. Nevertheless the USSR ran the world’s biggest illicit program right under the CIA’s nose. And they got away with it for years.

Developing malware is nowhere near as involved. Software engineers don’t need fermenting vats two stories tall. Offensive cyber technology tends to be small and easy to conceal. Agencies like the NSA can develop malware anywhere, with little or no logistical footprint, using compartmentalized cells of engineers hunkered down in unremarkable office spaces. Try spotting something like that with a spy satellite!

Furthermore, if a nation were to break a cyberarms treaty and deploy outlawed malware, spies would no doubt utilize anonymity technology in conjunction with anti-forensics to throw off investigators. Classified documents leaked to the press indicate that intelligence services, as a matter of standard operating procedure, use foreign commercial cover [7] to launch false flag operations [8]. The reason that we have definitive information about the authorship of Stuxnet [9] and Equation Group [10] malware is that U.S officials openly claimed responsibility.

Rather than trying to discourage other countries from building malware, why not promote national policies that work to render offensive technology inert? Cyber-attacks succeed on behalf of sloppy engineering. In part because hi-tech companies are allowed to treat security breaches as a negative externality. And also as a result of the NSA’s industry-wide campaign of subversion. In other words, poor cyber security is a matter of official policy [11]. Vulnerabilities persist because deep sources of wealth and power benefit from them.

The arms control mindset presumes the top-down worldview of cyber security a priori, where spies undermine our collective cyber security under the rubric of national security and CEOs sell substandard products on behalf of quarterly profits. Let’s reset American priorities to implement cyber-security from the bottom up so that everyone has access to relatively high levels of security.

Bill Blunden is the author of several books, including **“**The Rootkit Arsenal” and **“**Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware-Industrial Complex.” He is the lead investigator at Below Gotham Labs.

Share on Facebook Share
Share on Twitter Tweet
Report typos and corrections to 'corrections@alternet.org'. [12]
[13]

Source URL: http://www.alternet.org/news-amp-politics/cyber-arms-control-pipedreams-why-attempts-limit-malware-development-are-destined

Links:
[1] http://www.alternet.org/authors/bill-blunden
[2] http://alternet.org

[3] http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/

[4] http://www.nytimes.com/2015/02/26/opinion/arms-control-for-a-cyberage.html

[5] http://www.pbs.org/wgbh/pages/frontline/shows/plague/interviews/alibekov.html

[6] http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB61/

[7] http://foreignpolicy.com/2013/10/15/the-nsas-new-code-breakers/

[8] https://firstlook.org/theintercept/2014/02/24/jtrig-manipulation

[9] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[10] http://www.reuters.com/article/2015/02/16/us-usa-cyberspying-idUSKBN0LK1QV20150216

[11] http://www.alternet.org/print/news-amp-politics/latest-cyber-bank-robbery-demonstrates-govt-prefers-crappy-tech-security-its-own

[12] mailto:corrections@alternet.org?Subject=Typo on Cyber Arms Control Pipedreams: Why Attempts to Limit Malware Development Are Destined to Fail

[13] http://www.alternet.org/

[14] http://www.alternet.org/%2Bnew_src%2B