SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Case Western Reserve Journal of International Law

Volume 47
Issue 1 *Spring, 2015*

2015

# Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons

P. W. Singer

# STUXNET AND ITS HIDDEN LESSONS ON THE ETHICS OF CYBERWEAPONS

*By P.W. Singer* [1]

*In 2010, computer programmers around the world noticed a strange kind of cyber attack—although it had global reach, it was highly targeted and very sophisticated. A German team, led by Ralph Langner, figured out that the worm, now known as Stuxnet, specifically targeted certain operations related to the Natanz nuclear facility in Iran, causing the enrichment centrifuges to break down without any notice or apparent reason. As news of this new worm and its effects spread around the globe, the role of cyber attacks within the laws of war came into the forefront of discussions about the future of armed conflict. This article examines how Stuxnet changed the nature of cyber attacks and the ongoing discussion of where digital technology fits into the laws of war.*



## I. THE DIGITAL MYSTERY

Ralph Langner is a jovial fellow with a quick wit, whose sense of whimsy is perhaps best illustrated by the fact that he wears cowboy boots. Wearing cowboy boots shouldn't be all that notable, until one realizes that Ralph is not from Texas, but Germany, and is not a cowboy, but a computer specialist. Langner is also incredibly inquisitive. It was this combination that led him to play a role in the discovery of one of the most notable weapons in history; and not just cyber history, but history overall.

Since 1988, Ralph and his team of security experts have been advising organizations on the safety of large-scale computer system installations. Their special focus was industrial control systems, such as the Supervisory Control and Data Acquisition system (SCADA),

1. P.W. Singer is Strategist and Senior Fellow at The New America Foundation and co-author of the book *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2014) from which this article is derived. Further info at www.pwsinger.com . Special thanks to the Cyber Conflict Studies Association for its support.

that monitor and run industrial processes. SCADA is used in everything from the management and operation of power plants to the manufacture of candy wrappers.[2]

In 2010, like many other industrial control and cybersecurity experts around the world, Ralph grew concerned about the cyber worm of unknown origin that was spreading across the world and embedding itself in these control systems. Thousands of computers in places like India and the United States had been infected. But the bulk of the infections (roughly 60 percent) were in Iran. This led many experts to infer that either Iran had particularly poor cyber defenses for its SCADA-related programs, which made it more vulnerable, or a virus had initially targeted some site in Iran and, as one report put it, "subsequently failed in its primary purpose and run amok, spreading uncontrollably to unintended targets all over the world, and thus demonstrating how indiscriminate and destructive cyber weapons were likely to be."[3]

## II. STUXNET AND ITS CHARACTERISTICS

### *A. Getting Past Operating System Security*

Both turned out to be far from the case. Various teams of cyber experts from around the world began dissecting the code of this cyber worm, which became known as Stuxnet, and debates grew over its origin and targets.[4] Ralph and his team were curious, and the more they explored the code, the more interested they became in it. It was a wonderfully complex piece of malware like none the world had ever seen. It had at least four new "zero days" (previously unknown vulnerabilities), utilized digital signatures with the private keys of two certificates stolen from separate well-known companies, and worked on all Windows operating systems down to the decade-old Windows 95 edition.[5] The number of new zero days particularly stood out. Hackers prize zero days and do not like to reveal them when they don't have to. To use four at once was unprecedented and almost illogical given that one new open door is enough. It was a pretty good

2. P.W. SINGER & ALLAN FRIEDMAN, CYBERSECURITY AND CYBERWAR: WHAT EVERYONE NEEDS TO KNOW 115 (2014).

3. GEORGE R. LUCAS, JR., PERMISSIBLE PREVENTIVE CYBERWAR: RESTRICTING CYBER CONFLICT TO JUSTIFIED MILITARY TARGETS 14 (2011); NICOLAS FALLIERE, LIAM O MURCHU, AND ERIC CHIEN, W32.STUXNET DOSSIER, (2011).

4. William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), http://www.nytimes.com/ 2011/01/16/world/ middleeast/ 16stuxnet.html.

5. SINGER & FRIEDMAN, *supra* note 1, at 115.

sign that Stuxnet's makers had enormous resources and wanted to be absolutely certain they would penetrate their target.

Stuxnet also slipped by the Windows' defenses using the equivalent of a stolen passport. To gain access to the kernel, or operating system's control system, Stuxnet had to install a component that could talk to the kernel. The authors chose to target a device driver, a common tool that allows hardware devices to interact with the operating system. Windows uses a scheme of digital signatures to allow trusted hardware manufacturers to write device drivers that are trusted by the operating system. Unsigned drivers raise an alert for the user, while signed drivers do not.[6] The drivers in Stuxnet were signed by two real companies in Taiwan, indicating that the authors had access to the secret signing keys which were most likely stolen. Again, this is a rare style of attack: stolen signing keys are incredibly powerful, would have been well protected, and would be very valuable in any illicit market.

### *B. Stuxnet's Target*

Rather than being truly infectious, the malware's DNA revealed something even more interesting: Stuxnet was hunting for something in particular. As Langner delved deeper, he discovered that Stuxnet was not going after computers or even Windows software in general, but a specific type of program used in Siemens's WinCC/PCS 7 SCADA control software. Indeed, if this software was not present, the worm had built-in controls to become inert.[7] In addition, rather than trying to spread as widely as possible, as was the goal with past worms, Stuxnet only allowed each infected computer to spread the worm to no more than three other computers. It even came with a final safeguard of a self-destruct mechanism, which caused the worm to basically erase itself in 2012. Whoever made Stuxnet not only had a specific target in mind, but didn't want the code lingering in the wild forever.[8] This was a very different worm, indeed.

But what was the target? This was the true mystery. Here, Langner's background in working with industrial firms proved particularly useful. He figured out that Stuxnet was only going after a specific industrial controller, manufactured by Siemens and configured to run a series of nuclear centrifuges. But the target was not just any set of nuclear centrifuges; rather, it targeted only a cascade of

6. Randy Abrams, *Why Steal Digital Certificates?*, WE LIVE SECURITY (July 22, 2010, 4:39 PM), http://www.welivesecurity.com/ 2010/ 07/22/ why-steal-digital-certificates/.

7. Thomas M. Chen, *Stuxnet, the Real Start of Cyber Warfare?*, 24 IEEE NETWORK 2, 3 (2010), *available at* http://ieeexplore.ieee.org/ stamp/stamp.jsp?tp=&arnumber=5634434.

8. LUCAS, *supra* note 2, at 14.

centrifuges of a certain size and number (984) linked together. Not so coincidentally, this was the exact setup at the Natanz nuclear facility, a site suspected to be part of Iran's illicit nuclear weapons program.[9]

Things got especially tricky once Stuxnet found its way into this target (it was later revealed that the delivery mechanism was infiltration through Iranian nuclear scientists' own laptops and memory sticks). The attack didn't shut down the centrifuges in any obvious manner. Instead, it ran a series of subroutines. One, known as a *man in the middle*, caused tiny adjustments in the pressure inside the centrifuges. Another manipulated the speed of the centrifuges' spinning rotors, causing them to first slow down, then return to normal speed, destabilizing the rotors and ruining their work. On top of this, the malware would occasionally push the centrifuge speeds past the designed maximum. As a result, the centrifuges not only failed to produce refined uranium fuel, they frequently broke down and ground to a halt from the damaging vibrations caused by the various random surges. At other times, the machines literally spun out of control and exploded.

The effect, Langner wrote, was "as good as using explosives" against the facility. In fact, it was better. The victim had "no clue of being under a cyber attack." Stuxnet had been inside Iranian networks for over a year, but the nuclear scientists initially thought their facility was just suffering from a series of random breakdowns. The scientists just kept replacing the broken centrifuges with new ones, which would then get infected and break again.[10] Eventually, though, they wondered whether they were being sold faulty parts or were suffering from some kind of hardware sabotage. But the machines checked out perfectly every time, except for the fact that nothing was working the way it should.

### *C. What Made Stuxnet Different*

This was perhaps the most insidious part of Stuxnet: it was an integrity attack *par excellence*. Stuxnet didn't just corrupt the process; it hid its effects from the operators. It exploited not just technical vulnerabilities, but their all-too-human trust that the computer systems would accurately and honestly describe what was taking place. For a long period of time, the Iranian engineers didn't even suspect a cyber attack; their systems were air-gapped from the

9. Elinor Mills, *Stuxnet Expert: Other Sites Were Hit but Natanz Was True Target*, CNET (Feb. 14, 2011, 12:18 PM), http://www.cnet.com/news/stuxnet-expert-other-sites-were-hit-but-natanz-was-true-target/.

10. *See* Mark Clayton, *How Stuxnet Cyber Weapon Targeted Iran Nuclear Plant,* CHRISTIAN SCI. MONITOR (Nov. 16, 2010), http://www.csmonitor.com/USA/2010/1116/How-Stuxnet-cyber-weapon-targeted-Iran-nuclear-plant.

Web.[11] Moreover, up to this point, worms and viruses had always had an obvious effect on the computer, not the hardware. Eventually, the attacks had another effect: the Iranian scientists suffered low morale, under the impression that they couldn't do anything right; seventy years earlier a bunch of Americans had built an atomic bomb using slide rulers, and they couldn't even get their modern-day centrifuges to work. Overall, Langner likened the Stuxnet effect to the cyber version of "Chinese water torture."[12]

When Ralph Langer revealed his findings on his blog, the little-known German researcher quickly became an international celebrity. First, he had exposed a top-secret campaign of sabotage (later leaked in the American media to have been a collaborative effort between US and the Israeli intelligence agencies, known as "Olympic Games"), and second, it was a find of global importance.[13]

Beyond the operation itself and the impact it had on Iran or even US relations with other states or international law, Stuxnet stood out as something more. A new kind of weapon long speculated about but never seen, a specially designed cyber weapon, had finally been used. Prior cyber "attacks" had stayed within the digital realm, usually involving the theft, disruption, or manipulation of information.[14] Stuxnet did that, but caused something new, physical consequences. This made it like prior weapons in general, in that all weapons throughout history had caused physical damage. But it also took not merely cybersecurity but war itself into a new realm, being a weapon that was made of bits, rather than atoms. Like physical unmanned systems (such as drones), the worm separated the human point of decision geographically from the point of action, both physically (the "trigger" was pulled thousands of miles from the target in Iran), and, arguably, chronologically (the trigger was pulled months before). The worm was sent into contexts and locales that the sender couldn't expect to know. This meant that, by some definitions, Stuxnet was the first truly autonomous weapon.

Thus when it came time to weigh the new weapon, the debate diverged. Judith Donath of Harvard University described Stuxnet as a

11. Geoffrey Ingersoll, *US Navy: Hackers 'Jumping the Air Gap' Would 'Disrupt the World Balance of Power'*, BUS. INSIDER (Nov. 19, 2013), http://www.businessinsider.com/navy-acoustic-hackers-could-halt-fleets-2013-11.

12. *Better than Bunker Busters: The Virtual Chinese Water Torture*, LANGNER GROUP (Nov. 15, 2010), http://www.langner.com/ en/2010/ 11/15/better-than-bunker-busters-the-virtual-chinese-water-torture/.

13. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (Jun. 1, 2012), http://www.nytimes.com/ 2012/ 06/ 01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

14. *See* SINGER & FRIEDMAN, *supra* note 1, at 68–71.

demonstration of a new kind of weapon that could only get better: "The musket of cyberwarfare. What will be its rifle? Its AK-47? Its atomic bomb?"[15] Others worried that these new and better weapons would promote a new kind of escalation and global risk. "Stuxnet was the absolute game changer," wrote cyber thinker Mikko Hypponen. "We are entering an arms race where countries start stocking weapons, only it isn't planes and nuclear reactors they're stocking, but it's cyberweapons."[16] Still others were concerned of the opposite, that not enough people took notice of this "opening shot in a war we will all lose," says Leslie Harris of the Center for Democracy and Technology.[17]

## III. STUXNET AS CYBERWEAPON

Stuxnet was all of these things, perhaps, but it was also notable for another reason. This nasty little worm was a superb illustration of how ethics can be applied to cyberwar.

There is the popular notion that "all is fair in love and war," but the reality is that there are actually a series of strict guidelines that are supposed to shape behavior in war—what 1600s legal thinker Hugo Grotius called *jus in bello*, or law in wartime. Its two most prominent elements are proportionality and discrimination. The law of proportionality states that the suffering and devastation that one side causes, especially collateral damage to unintended targets, cannot outweigh whatever harm prompted the conflict.[18] In other words, if the other side stole your cow, you can't justifiably nuke their city. The law of discrimination maintains that all belligerent sides must distinguish between legitimate targets (e.g. a military post) and non-legitimate targets (e.g. civilians or wounded persons), and do their utmost to only cause harm to the intended, legitimate targets.[19]

Stuxnet stood out as a new kind of weapon in that it was designed to cause physical damage via cyber means. Its makers wanted it to damage targets in the real world, but only through action on digital networks. This was novel enough. But what really distinguished Stuxnet from traditional weapons was how small its physical impact was, especially in light of the intense stakes. The target was a nuclear bomb-making program, one that was already the target of diplomatic efforts and economic sanctions. While it is

15. *Id.* at 118.

16. *Id.*

17. *Id.*

18. Bruce Cronin, *Reckless Endangerment Warfare: Civilian Casualties and the Collateral Damage Exception in International Humanitarian Law*, 50 J. PEACE RES. 175, 176–77 (2013).

19. *Id.* at 175-76.

certainly arguable whether preemptive action against the Iranian program was justifiable, the Stuxnet attack makes the question of proportionality relevant. Stuxnet only broke nuclear centrifuges, which Iran had illegally obtained to conduct illicit research. Moreover, it neither hurt nor killed anyone. In comparison, when Israel attempted to obstruct Iraqi nuclear research in 1981, its forces dropped sixteen 2,000-pound bombs on a research site during "Operation Opera," leveling it and killing eleven soldiers and civilians.[20]

Discrimination also matters when judging the ethics of these attacks. At face value, Stuxnet seems incredibly indiscriminant. While limited in the scope of its attacks compared to prior malware, this was a worm that still got around. It infected not just targets in Iran but thousands of computers across the world that had nothing to do with Iran or nuclear research. Many lawyers see this facet of cyber weapons as proof of their inherent violation of "prevailing codes of international laws of conflict, as they go beyond just the original target and deliberately target civilian personnel and infrastructure."[21]

Yet this may be a wrong interpretation, outdated for the cyber age. While Stuxnet lacked discretion under the old way of thinking, its very design prevented harm to anyone and anything beyond the intended target. This kind of discrimination was something never previously possible in a weapon. As George Lucas, a philosopher at the US Naval Academy, wrote in an assessment of Stuxnet's ethics, "Unless you happen to be running a large array of exactly 984 Siemens centrifuges simultaneously, you have nothing to fear from this worm."[22]

In effect, judging the ethics of Stuxnet and cyber weapons more generally turns on which part of the story you care about most. Do you focus on the fact that this new kind of weapon permitted a preemptive attack and in so doing touched thousands of people and computers who had nothing to do with Iran or nuclear research? Or do you focus on the fact that the cyber strike caused far less damage than any previous comparable attack and that the weapon was so discriminating it essentially gave new meaning to the term? Are you a cyberweapon half full or half empty kind of person?

---

20. *See* Colin H. Kahl, *An Israeli Attack Against Iran Would Backfire—Just Like Israel's 1981 Strike on Iraq,* WASH. POST (Mar. 2, 2012), http://www.washingtonpost.com/pb/opinions/an-israeli-attack-against-iran-would-backfire--just-like-israels-1981-strike-on-iraq/2012/02/28/gIQATOMFnR_story.html; *Operation Opera,* 2EYES WATCHING UNIQUE BY NATURE (Feb. 17, 2012, 8:44 AM), http:// 2eyeswatching.com/2012/02/17/operation-opera/.

21. SINGER & FRIEDMAN, *supra* note 2, at 119.

22. LUCAS, *supra* note 2, at 15–16.

History may render the ultimate judgment of Stuxnet, however. As Ralph Langner put it, the fascinating new weapon he discovered "could be considered a textbook example of a 'just war' approach. It didn't kill anyone. That's a good thing. But I am afraid this is only a short-term view. In the long run it has opened Pandora's box."[23]

23. Mark Clayton, *From the Man Who Discovered Stuxnet, Dire Warnings One Year Later,* CHRISTIAN SCI. MONITOR (Sept. 22, 2011), http://www.csmonitor.com/USA/2011/0922/From-the-man-who-discovered-Stuxnet-dire-warnings-one-year-later.