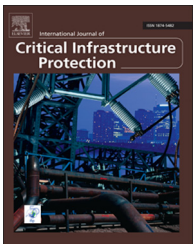
INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION 7 (2014) 244–246

Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Stuxnet and the vital role of critical infrastructure operators and engineers

Mark Hagerott

Center for Cyber Studies, U.S. Naval Academy, USA

Stuxnet – the famous computer worm that attacked Iran's uranium hexafluoride centrifuges – is a landmark in the history of cyber security and, very likely, in the history of military conflict. Yet, misconceptions about Stuxnet abound. Why? It seems that even after years of higher education and decades of specialization, very few people are able to approach a complex problem with a foundation of integrative knowledge and the essentials of computer science, industrial control systems, human factors, and military operations. Fortunately, one team of experts, led by Ralph Langner, has done the hard interdisciplinary work for us.

Ralph Langner went "viral" three years ago with his "TED Talk" on Stuxnet. In November 2013, he published an authoritative article, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. While the article is technically rigorous, it should be read by a broad audience: engineers; business executives; computer scientists; cyber security professionals and government officials. Quite frankly, anyone who is interested in the critical infrastructure should study Langner's work. *To Kill a Centrifuge* devotes considerable space to make accessible the complex technical details about Iran's centrifuges and their operation, and what Stuxnet may or may not have done to them. Most importantly, the article integrates technical findings with broader issues of operations, military doctrine, human factors, and workforce education and training.

First, some cursory background. Stuxnet is the name given to the malware that targeted Iran's uranium enrichment program. The malware was created by one or more unnamed nation states. Its primary goal was to target the Natanz uranium hexafluoride centrifuge facility, in particular, Siemens industrial controllers and the associated information technology and physical systems. Stuxnet is arguably the first documented case of malware that had destructive effects in the physical world.

Stuxnet will also go down in military history as malware that was deployed as a result of an intense dispute between nation states regarding nuclear proliferation. Instead of bombing Iran's centrifuge facility – as Israel did to Iraq's Osirak nuclear reactor in June 1981 – Stuxnet's creators (supposedly America and Israel) sought to inflict damage on the centrifuge facility using a clinical cyber weapon.

To Kill a Centrifuge provides the best, open-source explanation of Stuxnet, its purpose, and the likely sequence of actions that culminated in the destruction of centrifuges in Natanz. But lost in the public discourse and not clear in Langner's TED Talk, is that there were, in fact, two separate attacks perpetrated by Stuxnet.

To Kill a Centrifuge has riveting blow-by-blow descriptions of the two attacks. The first attack was a complex penetration and targeting of the centrifuge over-pressure protection system. The second attack, which occurred some years later and was much less complex and far more blatant than the first attack, targeted the centrifuge speed control system. The two attacks were independent, their outcomes neither coordinated nor controlled by the perpetrators after Stuxnet was in place. The article speculates that the perpetrators recognized the significance of launching the first cyber-physical attack in history. They were less concerned about the immediate effects of destroying centrifuges than sending a clear signal to Iran – and the world – about their technical prowess and the nature of cyber-physical warfare.

To be sure, *To Kill a Centrifuge* devotes considerable space to explaining the technical characteristics of Stuxnet and the targeted Natanz facility. But the article also offers invaluable insights into the social (i.e., human factors) aspects of the

E-mail address: hagerott@usna.edu

http://dx.doi.org/10.1016/j.ijcip.2014.09.001

Stuxnet attacks. It appears that the perpetrators opted not to induce an immediate, catastrophic failure of the centrifuges, although both of Stuxnet's attacks had the power to do so. Why? Because an aggressive attack and the subsequent failure of the centrifuges would have been recognized for what it was – an overt cyber hack. The hack would have elicited an immediate Iranian investigation and the securing of the remaining centrifuges. Iran also had thousands of spare centrifuges on hand and would have been able to restore the facility to full production within a few months. A blatant attack would have caused a temporary slowdown of the Iranian enrichment effort.

Instead of merely destroying centrifuges, Stuxnet primarily targeted humans – the Iranian operators and engineers at the Natanz facility. Why? To confuse the Iranians, erode their technical confidence, throw the enrichment program into confusion, create long-term inefficiencies, and cause major delays in the manufacture of weapons-grade uranium-235. Needless to say, these goals were largely achieved.

To Kill a Centrifuge is an exceptional analysis of an important cyber event. It stimulates deep insights that can inform industry executives, government officials and others who seek to understand the vulnerabilities and threats to industrial control systems and critical infrastructure assets. Some of the key takeaways are as follows:

- STUXNET will be copied and its variants will proliferate. Langner observes that a most dangerous misconception is that Stuxnet is so complex that copycat attacks will be few and far between. In fact, Langner opines that Stuxnet can be reworked to attack other systems and that a rework is simple enough to be done by lesser entities than nation states.
- Vulnerabilities are created by the automation and digitization of industrial control systems. A surprising insight concerns the limitations of automation and digitization. The Natanz centrifuge facility was derived from a Pakistani design that was stolen from the West by A.Q. Khan. However, the Iranians, in an effort to increase centrifuge efficiency and reliability, created a highly sophisticated digital control system for over-pressure protection that was an enabler for Stuxnet's cyber attacks.
- Human factors are as important as technical factors. Stuxnet most likely entered Iran's most sensitive Natanz facility when an Iranian engineer connected his compromised laptop to the control system. The laptop was probably compromised using a USB thumb drive.

As a former chief nuclear engineer in the U.S. Navy, I am convinced that human factors were the primary source of failure at Natanz and offered the greatest hope for early Iranian detection of Stuxnet. Why did the Iranian operators and engineers fail? And what might their failure teach those of us who design and operate critical infrastructure assets? Building on Langner's insights, I offer some additional observations.

The Iranian operators and engineers lacked cyber security awareness. The individual with the compromised laptop is ultimately responsible for introducing Stuxnet into the Natanx facility. This person was likely not on the attackers' payroll. This glaring failure of basic cyber hygiene in one of Iran's most sensitive facilities is shocking.

As unlikely as it may seem, the person with the compromised laptop may in fact have been acting on behalf of the attackers. Perhaps, this "insider" injected Stuxnet into the control systems in Natanz and attempted to mask the attacks. But even if this did, in fact, occur, the slow response and lack of vigilance on the part of the Iranian operators and engineers were egregious because they contributed to the persistence of Stuxnet and the severity of its impact. Stuxnet's second attack on the centrifuge rotors was simple and it completely disregarded operations security (OPSEC). Indeed, routine information assurance practices and log analysis would have revealed clear signs of Stuxnet.

Clearly, human shortcomings were in play. But why the lack of vigilance?

In *To Kill a Centrifuge*, Langner surmises that the Iranian operators and engineers did not have intimate knowledge of their systems, let alone the vulnerabilities created by the interactions of the various components of the systems. When industrial control systems are susceptible to hacking, it is incumbent on plant operators and engineers to master their physical systems, and understand the vulnerabilities and their potential impact. They should constantly ask (and answer) how a digital signal might cause physical damage and be on the lookout for signs, especially at the interfaces between the cyber and physical layers. Indeed, operators should pay particular attention to non-electronic, physical signals that reveal anomalies. George Lucas calls these signals "vibrations in the force".

Langner notes with exasperation that the Iranians failed in part due to a "failure of the ear drums". Stuxnet's centrifuge speed attack took the spinning centrifuges from their normal operational speed of 63,000 rpm up to 86,400 rpm and back down to 63,000 rpm. A month later, the same attack took them down to 120 rpm from 63,000 rpm, before bringing them back up to 63,000 rpm. These were not just "vibrations in the force". There would have been high pitched whines as the centrifuges revved up and then down; and vibrations as the centrifuges crossed the harmonic zone. The same would have occurred a month later as the centrifuges spun down, almost switching off and then revving up to full throttle. The noise would have been apparent; the silence more so.

In the final analysis, it does not appear that Stuxnet could have been stopped. Langner says that there are no technical "silver bullets" for Stuxnet and its variants. Anti-virus software is impotent because it is backward looking. Security patches may protect information technology systems and control systems, but they cannot fix zero-day plant vulnerabilities. Network segregation will not work, because it does not address the insider threat or an unknowing plant employee who bridges the air gap. The problem is fundamental to humans beings and the plants they build – in Iran, in the West, everywhere.

Stuxnet has changed the arcs of cyber security, critical infrastructure protection and human warfare. All of us – cyber

security professionals, scientists and engineers, critical infrastructure owners and operators, military professionals, government officials and concerned citizens – should read about Stuxnet, reflect on its implications, and hopefully take action. An excellent starting point is Langner's TED Talk. But do not stop there. Go on, and read *To Kill a Centrifuge*.

But if you are in charge of a critical infrastructure asset, urge your employees to go beyond the TED Talk and *To Kill a Centrifuge*. They must be ever aware of the failings of the hapless workers in Natanz and the vital role that trained operators and engineers play in critical infrastructure protection. More than anything else, they must know their machines and their vulnerabilities, and they should use all five (possibly six) senses to combat cyber attacks before they traverse the information technology and control system layers and wreak havoc on the critical infrastructure.

Dr. Mark Hagerott is a Distinguished Professor at the U.S. Navy Academy, Deputy Director of the U.S. Naval Academy Center for Cyber Studies, and co-founder of the U. S. Naval Academy's Forum on Emerging and Irregular Warfare Studies. A prominent researcher with interests in evolving technology, humans and war, Dr. Hagerott is a former Rhodes Scholar who has served as a chief engineer of a dual nuclear reactor plant, combat systems officer, U.S. Navy ship captain and Afghanistan war veteran.