FOUR KEY QUESTIONS ON WORMS AS A COUNTER-PROLIFERATION TOOL

Stephen J. Lukasik

The dialog below is inspired by the Stuxnet worm. On June 17, 2010 the Stuxnet worm was discovered. As a worm it was simply state-of-the-art, the theory of worms having been published by John von Neumann in the "Theory of Self-Reproducing Automata," in 1960, although his thinking went back to 1949. Worms originated in the U.S. in 1971, and were largely the work of computer scientists, identifiable through their research publications and public demonstrations. This state of affairs continued through the 1980s.

But the business changed in the 1990s. The number of PCs, i.e. targets, grew exponentially, Microsoft operating systems created a software monoculture, and the creation of the WWW in the early years of the decade further drove the number of targets *and* most importantly, the shift in the user population from a smaller number of more or less trusted users to billions of users to whom no degree of trust should have sensibly been imputed. In the 1990s it was quickly discovered that worms (more generally called malware, along with a number of other types of software such as adware and spyware) could do quite anti-social things, *and* that there was a market for writing malware. Malware went commercial, from script-kiddies and a cottage industry, to an underground multi-billion dollar industry supporting fraudulent activities.

The 1990s also saw the entry of states into the malware business, characterized by national security professionals studying cyber war and states creating formal cyber forces, such as the U.S. CYBERCOM, a subordinate command to STRATCOM. When one reads its official charter, one sees that the technical heart of CYBERCOM is NSA. The things that malware can enable, such as stealing personal information, is close to intelligence collection, so NSA at the heart of CYBERCOM is understandable.

Worms can do an impressive number of things. But what the creators of Stuxnet did was move in a new direction, targeting *industrial control (IC) systems*. For industrial control systems to control processes they must have an important component, Supervisory Control and Data Acquisition (SCADA) systems, the systems that collect the data so the control system can know what is changing and hence what control changes to effect. Worms have not been written by the commercial malware industry to attack such systems because there is no commercial market for them.

Attacking SCADA systems is the business of states. SCADA systems are at the center of infrastructure systems. Control of infrastructure is the functional equivalent of being able to destroy it. This is what cyber war is about. SCADA/IC systems of critical infrastructure are military targets. That their targets are, for the most part, privately owned complicates their protection since their private owners expect national security organizations to protect them from state attack.

The larger subject of cyber war is not the intent here, nor is the question of cyber deterrence. The use of malware against nuclear weapons facilities could be seen as an act of war. Its use against a treaty signatory in an enforcement role may be seen differently. Or, use of such software in voluntary monitoring roles, reporting to other treaty

signatories in real-time, could be a useful addition to inspection protocols. There would be a number of technical issues relating to data integrity and the provision for its secure and reliable transmission to clarify. Instead the focus here is on the narrower subject of the *feasibility* of the use of worms in a non-cooperative mode to intervene in the control of a state's nuclear weapon production facilities. If they are not feasible, we save ourselves the time of analyzing non-issues.

To surface the central issues, consider the following dialog:

Q: Is such a thing feasible?

A: That is what Stuxnet did to the Iranian enrichment facility at Natanz. And Stuxnet worked first time out of the box. While not perfectly, it was an effective demonstration of the feasibility of foreign access, through malware technology, to the computers that control the enrichment process, an otherwise difficult penetration target and a dangerous target for the use of force.

Q: Why the hedge about "not perfectly?" What did not work?

A: The characteristic of the net that got Stuxnet into Natanz made it easy for Stuxnet to get into other Seimen's software-dependent facilities as well. Consequently Stuxnet spread too far too fast, making it inevitable it would be discovered. Since Stuxnet was supposed to stay hidden and do its work over a period of years, its impact was limited to the destruction of some thousand Iranian centrifuges

Q: So does this mean worms are feasible but not reliable?

A: Not clear. That leads to **Key Question #1. Can one construct a stealthy SCADA/IC attack worm that is not a blunderbuss, but like a silenced sniper rifle?**

Q: What is your opinion?

A: The first of anything rarely achieves its theoretical maximum performance. Remember Moore's law. Information technology changes rapidly. Eighteen months is a big deal. The technical challenge is to get the worm into the target computers and have it function without being detected. An enrichment cascade that is connected, directly or indirectly to the global communications network is easier to get into than one that is not. Absent such a connection, as was, presumably the case, with Stuxnet in Iran, the more problematic is the issue.

Nevertheless, the counter proliferator may still have opportunities: insiders, vendor supply chains, and RF techniques come to mind. No technique is guaranteed. The less watchful the proliferator, the more often the penetration can be attempted without penalty to the counter-proliferator. Nanotechnology employed for penetration devices can possibly be useful.

Q: But even if you do create a stealthy worm, won't the target nation eventually wise up from the fact that it has a production facility that has little or no output?

A: Yes, but what is the target nation to do? It can start over, writing all the control software itself, and maybe redesigning its centrifuges so the worm writer does not have enough information to know how they operate. No legacy software can be relied on. This would be an expensive and time-consuming effort, because it is not only the control system, but all the supporting software infrastructure down to new printer drivers, compilers, and spreadsheets. The proliferator will recognize he must be good at detecting worms. This is the essence of information technology, hardware and software. It changes rapidly. The attacker has to develop better and better worms and the defender has to develop better and better worm detectors. It is a dynamic resource battle over work factor, just as in cryptography. This leads to **Key Question #2. How much resource can the proliferator put into defense vs. how much resource can the counter-proliferator put into offense?**

Q: OK, so sometimes the proliferator is ahead and sometimes the counter-proliferator is ahead. Is this just a software arms race?

A: Yes. Welcome to the real world. But return to the time issue mentioned above. Suppose this seesaw battle goes on with the proliferator having a hard time getting ahead, or keeping up, or breaking out. The counter-proliferator buys time. This leads to **Key Question #3. What is the time worth? Is it enough to allow other political tools to be brought to bear on the proliferator?**

Q: I see that, but it is a bit of a let-down. Worms do not have a potential as silver bullets?

A: Like all technology, there is always the risk of failure, unintended consequences, a newer hotter biscuit. Cyber tools can be part of a counter-proliferation program, presumably international in scope. Worms are cost-imposing tools, where the cost is the cost of cyber defense, the cost of redesign of processes, and the cost of windows of opportunity.

Q: I'm discouraged because it does not look like Stuxnet is going to help me with Iran. We tried it and it did not stop them in their tracks. Now they know about our capabilities. We have lost the advantage of surprise. Iran has formed a Cyber Police Force to make it tougher for us in the future. The counter-proliferator has to start over, this time making stealthy worms, and get them into closed areas that will be even harder to penetrate in the future. So is thus just another technology dream to be revisited in ten years?

A: The situation not quite that bad, but it is good that you recognize the problems and see what the key questions are if you are to avail yourself of the cyber tool. We saw in the Cold War there were major technology and strategic posture changes between 1949 and 1989. The offense–defense balance changed but never in a direction that overwhelmingly favored one side. Political confidence building measures were adopted and inspection procedures to enforce agreements established.

There is, however, a difference between halting a well-advanced program and controlling one just starting. The Iranian program goes back to the Shah, and Iran has maintained a steady course to nuclear weapons. Iran will not be the last proliferator. Worms to attack nuclear infrastructure are a tool under development. The state of the Iranian program provides a incentive to develop cyber attack technology, one that is ultimately defensive in nature. Since the U.S., and the rest of the world, needs an overwhelming good reason

to do anything, cyber counter-proliferation is as good a reason to get to work as any. This points up **Key Question #4. What is your strategic goal? Is it to drive all nuclear weapon production to zero? Or is it to increase the entry barrier to new nuclear weapon states? Or to buy time for other for other forces to be applied that together may tip the balance in favor of the counter-proliferator?**

Q: There has been no mention so far of chemical reprocessing plants for plutonium weapons. Can't they be attacked by cyber tools as well?

A: Yes, reprocessing plants depend on SCADA/IC software as well. There is an important difference between attaching enrichment facilities and chemical reprocessing facilities. Long-term damage to centrifuges is possible to interfere with the HEU production rates. In the case of reprocessing plants, there are far more dangerous levels of radioactivity involved. Attacking them will result in higher risks of collateral damage.

Q: So are you sanguine about the prospects of cyber tools to aid in counter-proliferation?

A: Yes. As a card-carrying technologist who assisted in the birth of the ARPANET in the 60s and 70s, and a member of the military-industrial complex for 60 years, I believe we can use cyber technology to advantage, in conjunction with other hard and soft power assets, for counter-proliferation. But there is no guarantee of success. Cyber technology is new to the counter-proliferation problem. It can do some good, more in the case of "easy" proliferators and less in tougher cases.