All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Open CyberWar

It appears that the US is now admitting, through the usual back channels of the media, that it has started to engage in open cyber warfare. This with the apparent admission that Stuxnet was a US operation.[1] The failure to immediately disclaim the leak and media stories related to it is proof enough for most, and in today's World, as close to an admission as there is. To be clear, the nation-states of the world have long been engaged in information warfare, in fact this has more or less always been true. But a change has come, and with this change, there may be a frightful price to pay.

What is CyberWar?

In information warfare, targets include things like intellectual property, business information, and state secrets. They are strategic and tactical targets that lead to competitive shifts, and the effects are almost entirely indirect. But cybernetic systems are quite different. They are physical systems that use feedback for control.[2] To the extent that this feedback can be made to work against the objective function of the system rather than for it, such systems have a tendency to fail catastrophically. That's another way of saying, they blow up.

In other words, you get direct kinetic effects from memetic weapons. In a cyberwar, the systems that support modern civil society are subject to destruction, putting the civilian population directly at risk. At risk to the same sorts of effects as we have seen in historic wars from loss of electrical power, fuel supplies, water supplies, destruction of the financial system, communications system, the Internet, and the damage to commerce and public safety that all come together in this package.

The “good” part is that large numbers of people aren't directly killed by explosions. The bad part is that they are made to suffer the consequences of the breakdown in society that happens when government and governance are no longer. While many people seem to believe that this could be a good thing, in that people will learn how to live off the land again, only the strong will survive, and it will potentially help to solve the population problem, culling the herd is likely to cull much of modern society, which is where I live. So as a purely personal matter, I'm against it.

The barriers have been removed – and a treaty won't likely happen soon

The history of treaties would suggest that they don't happen till they are demonstrably needed by all sides. Once a major nation-state starts to engage in a form of warfare, they have let loose the dogs of war. Unless immediately challenged and shunned by the World community, the new form of warfare becomes the standard by which we all live and die. And that is what has apparently just happened. Cyber attack is no longer “hackers” or “criminals” or “corporate malfeasance”. It is now and for the foreseeable future, military weaponry – subject to all of the things that go with that unique distinction.

[1] D. Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran”, 2012-06-01, NY Times

[2] Norbert Wiener, “Cybernetics”, 1948

Weapons are subject to all manner of constraints, and all manner of funding. The Stuxnet weapon was unleashed on Iran and accidentally let loose on the rest of the World. Which is to say, the US appears to have failed in its policy of limiting collateral damage. And worse yet, the damage came to, among others, its own interests. Fratricide in cyberwarfare seems certain unless and until we learn to control our weapons. And frankly, offense takes precedence in warfare, and that likely means gobs of money and effort in the attack side, and far less in the defense side. And this is not the first time. Offensive efforts in information warfare far outstripped defensive efforts for the last half of the 1900s, and led us to the system of vulnerabilities we now live with. And things are not getting better.

Escalation

The next step is the inevitable escalation. There is no choice at this point. Every technically advanced nation state that wants to continue to exist has little choice but to learn to attack its neighbor, if only as deterrence. The new weapons of cyberwar do not favor the Western nations. In fact, it's the opposite. Western civilization is the most dependent on cybernetic systems, and has spent much of the last decade moving away from the safety of classic control systems toward the riskier, and slightly more efficient under ideal conditions, general purpose computing applied to control systems. Many if not most of these systems are literally so full of holes that they cannot be patched. Replacement cycles that used to be 30+ years are rapidly moving to the 3-5 year time frame of information technology, with its constant need for updates and lack of careful systems design. The “sell it then fix it” approach that has dominated computing for the last decades is practically guaranteed to fail.

When a single computer system failure can cause catastrophic failure of the cybernetic system, redundancy is needed. But redundancy is far less effective when the components have common mode failures and common interdependencies. And that is what is produced in large part in modern control systems using general purpose computing. Escalation of offensive cybernetic warfare will likely bring the same level of complexity to defending cyber systems as it has brought to defending common computer systems. And that is potentially catastrophic in war. Today there are thousands of new computer virus variants released into the World every day. And these are being exploited, in large part, merely to steal hundreds of millions of private records and at least tens of billions of dollars every year. But when every credit card number stolen becomes another control system destroyed or disabled, the consequences may be truly profound.

Conclusions:

The era of innocence seems to be over when it comes to cybernetic systems. Warfare is now on its way, and not the warfare of someone knowing your bank account number or sending email in your name to your social circle. Cyberwar is information technology with physical effect used to destroy the capacity of other nation states. Whether through surrogates or more direct acts, the World will likely start to see the real damage done by these methods in the near future. It is now time for government to act definitively and decisively in the defense of the nation state – all governments – if they wish to continue to bring prosperity to their people. Industry cannot and will not provide for the common defense – that is the role of government. And the best defense is not a good offense when there is a fundamental differential in effect. The only defense is a good defense, and only government can fix what it has wrought.