# STUXNET AND THE POISONS THAT OPEN YOUR EYES

Playwright August Strindberg wrote, "*…There are poisons that blind you, and poisons that open your eyes.*"

We've been blinded for decades by complacency and stupidity, as well as our trust. Most Americans still naively believe that our government acts responsibly and effectively as a whole (though not necessarily its individual parts).

By effectively, I mean Americans believed their government would not deliberately launch a military attack that could affect civilians — including Americans — as collateral damage. Such a toll would be minimized substantively. Yesterday's celebration related to the P5+1 interim agreement regarding Iran's nuclear development program will lull most Americans into deeper complacency. The existing system worked, right?

But U.S. cyber warfare to date proves otherwise. The government has chosen to deliberately poison the digital waters so that all are contaminated, far beyond the intended initial target.

There's very little chance of escaping the poison, either. The ubiquity of U.S. standards in hardware and software technology has ensured this. The entire framework — the stack of computing and communications from network to user applications — has been affected.

- Network: Communications pathways have been tapped, either to obtain specific content, or obtain a mirror copy of all content traveling through it. It matters not whether telecom network, or internal enterprise networks.

- Security Layer: Gatekeeping encryption has been undermined by backdoors and weakened standards, as well as security certificates offering handshake validation between systems.

- Operating Systems: Backdoors have been obtained, knowingly or unknowingly on the part of OS developers, using vulnerabilities and design flaws. Not even Linux can be trusted at this point (Linux progenitor Linus Torvalds has not been smart enough to offer a dead man’s switch notification.)

- User Applications: Malware has embedded itself in applications, knowingly or unknowingly on the part of app developers.

End-to-end, top-to-bottom and back again, everything digital has been touched in one layer of the framework or another, under the guise of defending us against terrorism and cyber warfare.

Further, the government watchdogs entrusted to prevent or repair damage have become part and parcel of the problem, in such a way that they cannot effectively be seen to defend the public’s interests, whether those of individual citizens or corporations. The National Institute of Standards and Technology has overseen the establishment and implementation of weak encryption standards for example; it has also taken testimony [PDF] from computing and communications framework hardware and software providers, in essence hearing where the continued weak spots will be for future compromise.

The fox is watching the hen house, in other words, asking for testimony pointing out the weakest patches installed on the hen house door.

The dispersion of cyber poison was restricted only in the most cursory fashion.

- Stuxnet’s key target appears to have been Iran’s Natanz nuclear facility, aiming at its SCADA equipment, but it spread far beyond and into the private sector as disclosed by Chevron. The only protection against it is the specificity of its end target, rendering the rest of the malware injected but inert. It’s still out there.

- Duqu, a “sibling” cyber weapon, was intended for widespread distribution, its aims two-fold. It delivered attack payload capability, but it also delivered espionage capability.

- Ditto for Flame, yet another “sibling” cyber weapon, likewise intended for widespread distribution, with attack payload and espionage capability.

There could be more than these, waiting yet to be discovered.

In the case of both Duqu and Flame, there is a command-and-control network of servers still in operation, still communicating with instances of these two malware cyber weapons. The servers’ locations are global — yet another indicator of the planners’/developers’ intention that these weapons be dispersed widely.

Poison everything, everywhere.

But our eyes are open now. We can see the poisoners fingerprints on the work they’ve done, and the work they intend to do.

After their poison effectively damaged the viability of Natanz uranium refinement program, they will claim victory with the Iranian agreement on nuclear proliferation — yet at what long term price? Not unlike the early treatments for syphilis requiring the patient’s exposure to mercury, those who stood by as therapists and visitors must have been exposed on a limited basis to the chemical neurotoxin, collaterally damaged.

Likewise, Stuxnet’s collateral damage remains, a toxic cure waiting to realize maximum potency on targets which were not the primary focus of Stuxnet’s first and second deployments.

Code lies waiting for a patch or update to refresh it, ready to be relaunched for aims that may not serve the original planners. Holes remain open, serving as doors for some other entity’s purposes — perhaps another nation-state’s hostile attack, perhaps a criminal smash-and-grab, or a massive extortion attempt.

Not to mention the loss of trust among global partners whose civilian technology has been put at risk at scale undetermined, for a period of time unclear.

Or worse: whoever ordered, planned, and wrote the Stuxnet family of cyber warfare weapons wanted assurance that any other attempts to subvert their will could be dealt with in the same fashion that Stuxnet damaged Iran. There is no trust, just hegemonic cyber power. There is only a technological poison waiting for the day when its manufacturer decides to re-arm the toxic payload — a cyber weapon held to the heads of every nation-state, every corporation, every individual who relies on the existing, compromised computing and communications framework.

If Iran was successfully cowed by systematic damage to its nuclear development program and more, how easily will other nation-states be pressured into compliance with but a bit of fresh cyber poison? Will the next deployment be restrained as the second wave of Stuxnet, or will it be as ruthless as Stuxnet’s earlier evil twin was intended to be?

Open your eyes.