The Programmable Diplomatic Kill Switch

David Davidian

January 20, 2017

If indeed “War is a mere continuation of policy with other means” [1] the metaphoric kill switches that have made their way into strategic weapons by arms manufacturers give Clausewitz's nearly two-hundred-year-old observation new meaning. The ability of states that manufacture complex strategic networked weapons systems to simply turn off or at least partially disable such systems, on demand, is not really new. This capability is not simply to insure such weapons cannot be turned and used against states that manufacture them. It can and will be used when it is in the interest of third-party states to modulate a conflict. International relations could be steered down a path that was once traveled down by surrogates of superpowers. When systems not even designed to be rendered useless, such as Siemens' programmable logic controllers running electro-mechanical processes in factory automation (by targeted cyber weapons, such as Stuxnet) one can just imagine the possibilities that are available when remote disabling designed into weapons systems.

Surely, a kill switch is not a marketing feature, nor will one have its tutorial in the training manuals of the U.S. FA-18 Hornet's Target Acquisition System, Israel's Hermes and Heron UAVs (Unmanned Aerial Vehicles, or drones), or in Russia's Iskander guided ballistic missile, among other systems. Such compromised access is made through backdoors, allowing unauthorized remote access to the computer control hardware. These backdoors are not hacked into but rather are designed into the system, analogous to the Trojan Horse tale of subterfuge.

We are not talking about the future. When the U.S. sold FA-18 jets to Australia three decades ago, they would not supply the system codes necessary to acquire enemy targets the Australians wanted them to. These jets would only lock on targets the U.S. would allow [2]. Subsequently, the Australian military developed their own Electronic Warfare Self Protection, a Radar Warning Receiver known as ALR-2002 [3]. It has been also claimed that Australian programmers discovered the codes the U.S. would not provide them [4], but both of these indigenous efforts might be the same although announced and interpreted differently. The Australian Defense Minister at the time noted "*The radar of our Hornet could not identify most of the aircraft in this region as hostile … so our frontline fighter could not shoot down people who might be the enemies in this region*" [5]. By 2006 Australia's ALR-2002 project was being phased out in favor of Raytheon's ALR-67 (V3) as this unit provided necessary access to radar signatures the Australians required and it was fully operational, whereas the ALR-2002 was still in its qualification stage. For fifteen years, the U.S. arbitrarily denied an ally access to full system capabilities.

There have been reports [6] that during a specific politically contentious period between Turkey and Israel, 2014 or before, Israel sent a strong message to the Turks through a surrogate, Azerbaijan, when some of Azerbaijan's Israeli-manufactured UAVs were unexpectedly unable to launch. This would not be surprising as Israel's Elbit weapons manufacturer and other IAI (Israel Aerospace Industries) have tended to use unified UAV control and data centers, robustly connected via networks and satellites [7].

On September 6, 2007, when the Israeli Air Force destroyed a purported Syrian nuclear research facility, Syrian early warning radar wasn't just jammed but it appears their entire network was disabled to such an extent that the Syrians never saw the Israeli jets violate Syrian air space. As with the Azerbaijani incident, no official mission report was made public. Much of the Syrian military only knew of the events after the facility deep inside Syria was destroyed. It seems that a combination of techniques was used, including speculation that the Israelis were able to incapacitate key pieces of computer technology using Syria's own command and control infrastructure, including algorithm injection and infecting systems that may have actively compromise CPU function (Central Processing Unit or microprocessor). The latter is conjecture in this case, although not without precedent. The French manufactured CPUs with the ability to be shut down remotely when used in military equipment they export [8]. Spiegel [9] wrote that a Syrian official, during a 2006 trip to England in late 2006, frivolously provided access to his laptop, allowing Israeli agents to place a Trojan Horse malware on the laptop, eventually revealing the inner workings of the purported nuclear facility. Some details can be found in the November 26, 2007, Aviation Week and Space Technology article [10] and any role the U.S. technology may have played.

Some argue that it is costly and even a security risk to incorporate kill switches in high-tech weaponry [11]. However, such an argument loses its price-performance claims as the systems move from anti-tank weapons and shoulder launched surface-to-air missiles (such as Stingers) to strategic drones and ballistic missiles. Besides, it is well-known that the U.S. and other major nuclear powers install safeguards not only on their nuclear arsenal (known as Permissive Action Link) but also on items such as jets and strategic bombers. For example, upon receiving a series of codes embedded in part of its target acquisition system, an F-16 will shut off its weaponry if part of its return signal information includes codes determined to be coming from a targeted U.S. asset. Its radar may send a coded pulse and listen for a specific response. This is nothing new and is used to prevent such aircraft from attacking a real U.S. piloted aircraft or other military facilities. This capability extends to other large weapons manufacturing states.

The following is taken verbatim from The Economist's Technology Quarterly, November 30, 2013 [12]:

> *“Kill switches” or “backdoors”, as these features are sometimes known, have so far been associated with expensive weapon systems that must send and receive data to operate. David Kay, America’s most senior arms inspector in post-Saddam Iraq, has noted that one of the reasons why Russia’s best air-defence systems have not been installed in Iran is probably because the Iranians fear that Russia might be capable of countermanding missile launches against certain countries’ aircraft. Now similar “override” systems are being applied to small arms, too.”*

Major strategic weapons manufacturers would be remiss if they did not add such a capability to control the use of their weapons.

It has been suggested that military-class GPS navigation or a time limiter be added to tactical weaponry, allowing their use in a limited geographic area and only for certain time periods, or both. A satellite overhead could reset the weapon's timer with a stroke of a remote keyboard. If this is within the realm of possibility, the same mechanism easily becomes a kill switch, thus turning on or off the ability to exercise the weapon effectively. Worse, such a capability could permanently disable on-board computer circuitry. Even certain cell phones turn into bricks if lost or stolen. A 2011 Brookings study [13] notes how UAVs are basically networked flying computers and "*on-board computer systems on drones can be equipped with kill switches that could be tripped remotely if the drones go missing*" and, thus, can easily be turned into inoperable bricks by remote fiat.

Claims of disabling or altering CPU function do come with empirical evidence. A state-of-the-art Intel- or AMD-powered Windows computer comes with the ability to update its microcode. The microcode is used to translate, internally within the CPU, the individual instruction in the running software into actual operations within the CPU. Such operations could be arithmetic, logical, and/or other. This means there is access to core internals of these microprocessors, regardless of "guaranteed" safeguards. In addition, most integrated circuits over the past 25 years or so can be tested as a functional unit using JTAG (Joint Test Action Group) pins. Further, these and similar JTAG lines are available on motherboards. JTAG offers access to the internals of integrated circuits, since its function is to test subsections of finished products. Unless these JTAG lines are physically disconnected from the user, they provide sources of backdoor access.

A very convenient integrated circuit known as an FPGA (Field Programmable Gate Array) is specifically designed to power-up without any real operational capability; it simply awaits initialization, programming, and loading of other operational procedures into the FPGA upon boot-up. In military systems, every effort is made to verify and securely feed proper instructions into the FPGA, but many of these FPGAs have been subcontracted to entities outside the borders of weapons manufacturing states, which is asking for trouble. A case in point is the

American-designed, but Chinese-manufactured, ProASIC3 FPGA (also known as PA3) by Actel (now Microsemi) used in products spanning automotive to aerospace to U.S. military applications, which was purported to have a deliberate backdoor. This was demonstrated by researchers at the University of Cambridge and Quo Vadis Labs in England [14]. Some dispute a deliberate intent, claiming that no evidence has been brought forth that it was a intentional design-in [15]. Others claim backdoors are everywhere, waiting to be exploited [16].

Former U.S. counter-terrorism czar, Richard Clarke, stated in the Smithsonian Magazine [17] that an unknown majority of electronics made in China may have backdoors. This may be an extreme view, but he also suggested in memos to national security advisor Condolezza Rice on January 25, 2001 and September 4, 2001 that something on the scale of 9/11 may be in the planning. [18]

In any case, since claims of backdoors, malware, and CPU accesses peaked in 2012, U.S. government agencies have intensified the search for and programs to detect such traps, backdoors, kill switches, etc. Such activity began even as early as 2005 and 2007 [19]. By mid-2013, it was reported in Security Affairs that “spy agencies reportedly have a long-standing ban on Lenovo PCs due to backdoor vulnerabilities”, stating “the research allegedly documented the presence of hardware and firmware backdoor vulnerabilities in Lenovo chips” [20].

It turns out that Intel, the maker of the most popular series of microprocessors in the world, the x86, has added a second tiny processor to its latest chipsets [21]. The prevailing explanation for the function of this added processor, which cannot be seen by the main CPU or the operating system, is to aid in remote management. This is an enhancement to an older subsystem called Intelligent Platform Management Interface (IPMI). However, Intel's Management Engine (ME), a 32-bit ARC processor, in conjunction with Intel's Active Management Technology (AMT), runs in the background even when the system is powered down, has the ability to monitor network traffic with its own dedicated network stack, runs its own firmware secured with 2048-bit RSA encryption, and has access to system RAM [22]. While probably not designed to be a backdoor, it can be used as one [23].

The diplomatic nature of this metaphorical kill switch could determine the outcomes of conflicts. Of course, such manipulation of military hardware has its limits. Military secrets are most fleeting and, as such, kill switches must be used in a manner that would make their effects appear somewhat innocuous. As demonstrated by the effort put forth by the Australians on their F-18s, it will only be a matter of time before the capabilities of kill switches are overcome. In response, the controlling "diplomats" may simply increase the errors in the trajectory of projectiles, slow down the sampling rate of sensors, etc., lest the military-industrial complexes of the world lose their markets to indigenous development.

David Davidian is an Adjunct Lecturer at the American University of Armenia. He has spent over a decade in technical intelligence analysis at major high technology firms.

[1] "Der Krieg ist eine bloße Fortsetzung der Politik mit anderen Mitteln" Everything You Know About Clausewitz Is Wrong

[2] Beazley tells of US code crack

[3] Economics of War and Peace: Economic, Legal, and Political Perspectives, Ben Goldsmith, Jurgen Brauer, Emerald Group Publishing, 2010. Chapter 4: Arms Export Controls and the Proliferation of Weapons Technology, pages 59-66

[4] Australia 'cracked top-secret US jet fighter codes'

[5] See ref #3, Economics of War and Peace , page 63

[6] No hard documented empirical evidence has been presented to this author to conclude causation. However, the correlation between the near absence of Israeli-manufactured Azerbaijani drone sorties with the peak in political tension encountered by Israel (in at least one specific case) is rather interesting.

[7]   Hermes™ Universal Ground Control Station (UGCS) and UAV command, control & communications

[8] High-tech weapons sow fears of chip sabotage and New Technique Detects Hardware Trojans , many others such as, The Hunt for the Kill Switch

[9] How Israel Destroyed Syria's Al Kibar Nuclear Reactor

[10] Aviation Week and Space Technology

[11] The Case for Kill Switches in Military Weaponry

[12] Kill switches and safety catches

[13] Cyber-Physical Attacks and Drone Strikes: The Next Homeland Security Threat

[14] Breakthrough silicon scanning discovers backdoor in military chip

[15] Experts dispute threat posed by backdoor found in Chinese chip

[16] Back Doors Are Everywhere

[17] Condo Lied: Declassified memo from Clarke

[18] Richard Clarke on Who Was Behind the Stuxnet Attack

[19] Defense Science Board Task Force on High Performance Microchip Supply and DARPA “TRUST in IC’s” Effort

[20] Spy agencies ban on Lenovo PCs due to backdoor vulnerabilities

[21] Intel x86s hide another CPU that can take over your machine (you can't audit it)

[22] Intel ME Secrets; Hidden Code in your Chipset and How to Discover What Exactly it Does

[23] Is the Intel Management Engine a backdoor?