**Cyber Kinetic: The Next Step in Warfare**

**Zachary E. M. Burson**

**University of Maryland University College**

**Feb 2018**

In the film *The Italian Job (2003)*, Lyle (Seth Green) hacks into Cyber Physical Systems (CPS) in order to gain control of traffic lights and Closed-Circuit Television (CCTV). He disables monitoring and access by traffic engineers, causes major vehicle collisions, and creates a gridlock in key areas for the team to continue their attack. This scene could have been the inspiration for the 2006 hack of Los Angeles city traffic system (Ivezic, 2017), where traffic was at a stand-still for days in congested areas. As we look to make our daily lives easier by integrating smart technology and CPSs into The Internet of Things (IOT), we often don’t realize that we might be putting ourselves at risk of Cyber Kinetic attacks. According to Scott D. Applegate, “Kinetic Cyber refers to a class of cyber attacks that can cause direct or indirect physical damage, injury or death solely through the exploitation of vulnerable information systems and processes...Generally, the main targets for kinetic cyber attacks are cyber physical systems (CPS).” (Applegate, 2013). Growing amongst conventional cyber threats, Cyber Kinetic attacks strive to be one of the most destructive, controversial threats with widespread interest from security analysts, terrorist groups, and even nation-states.

Starting in 1982 and slowly growing in popularity, Cyber Kinetic attacks are becoming progressively employed, seeking to create devastation and gain political clout. One of the most spectacular, comprehensive attacks in Cyber Kinetic history was claimed by a former U.S. CIA operative in 1982 (Ivezic, 2017). After gaining intelligence of Soviet interest to update gas pipeline software, the U.S. hatched a plan to sabotage the sought-after pipeline assets. The CIA embedded code into the software with an attack we now call a logic bomb. The U.S. then tricked Soviets into stealing the repurposed program, setting off the logic bomb after four or five months, increasing the pressures of the pipeline, ultimately causing a catastrophic explosion. While this attack was one of the first of its kind, the idea sparked interest in nation-states, hackers, and terrorists, and pursued through the next three decades.

“Another, more well-known example, is the Stuxnet worm which caused Siemens Programmable Logic Controllers (PLCs) in an Iranian nuclear facility to spin centrifuges fast enough to damage them, setting back the Iranian nuclear program by years.” (O'Hara, 2015). This meticulous 2009 targeted attack was believed to have been created by U.S. Central Intelligence Agency (CIA) and Israeli government officials. The attack may have destroyed as much as 10% of uranium enrichment centrifuges from Iran’s Natanz Nuclear Power Plant (Ivezic, 2017). The worm was thought to have been employed via a personal USB device, and replicated itself until it found its target on a Supervisory Control and Data Acquisition (SCADA) network. It then created a backdoor for operatives to spy on the network, gather information, and take control of the centrifuges, all while providing false-positive reports to the network overseers. This intricate attack made waves in the realm of cyber warfare, it set the benchmark; Iran targeted U.S. banks in retaliation. As stated by Jeffrey Carr, founder and CEO of Taia Global, “The takeaway is that nation-states are spending millions of dollars of development for these types of cybertools, and this is a trend that will simply increase in the future.” (Kushner, 2013).

In 2014, a German steel mill became another target of a destructive attack. Marin Ivezic states “Once they penetrated the corporate system, they worked their way into production management software and took control of most of the plant’s operations. They disabled sources of human intervention on the systems and targeted high value equipment, including a blast furnace whose shutdown controls they disabled, overheating it until it was ruined.” This attack, like the Soviet pipeline explosion and Stuxnet, caused massive damage to industrial equipment, rendering it useless until it was repaired.

Today, we aim to reduce the many vulnerabilities in our advanced technologies such as 3D printers, drones/unmanned aerial vehicles (UAV), medical equipment, firearms, self-driving cars, and aircraft. Many security researchers are aiming to identify and publicize possible areas of concern in CPSs. In the article *Using 3D Printers as Weapons*, Mark Yampolskiy et al. expose many possible vulnerabilities associated with 3D printing and manufacturing systems. One of their fears is that with increased usage of 3D printing for industrial equipment, it is possible for hackers to gain access to the CPSs and diminish the structural integrity of the components being built. Yampolskiy et al. writes “For example, an adversary can compromise a 3D printer in order to manipulate the mechanical properties of manufactured parts. If the manufactured parts are used in jet engines or in other safety-critical systems, they could endanger human life, disrupt critical infrastructure assets and produce significant economic and societal impacts.” (Yampolskiy, et al., 2016). Another vulnerability could allow hackers to exploit the system to cause an explosion of the additive manufacturing equipment used to produce the 3D printed objects by mixing highly flammable or explosive materials in the source material during the manufacturing process (Yampolskiy, et al., 2016).

We also face vulnerabilities in our UAV and drones. While the military has been using UAVs since the early 2000s to gather intelligence provide attack capability, UAVs are being adopted in consumer technology as well. Personal drones have become a hot commodity on the market for entertainment and photography, while industrial drones are becoming more popular as well; delivering goods and inspecting critical infrastructure for damage. There is good intention in these UAVs that could be compromised if not protected. Vahid Behzadan explains that it is possible for attackers to manipulate or misuse sensory input functions to misguide or disable sensors, causing the UAV to return-to-base, resulting in a denial of service that could be crucial to military intelligence. He also states that it is possible to disable or interfere with Air Traffic Control Collision Avoidance systems that detect aircraft collisions (Behzadan, 2017). With this in mind, an attacker may be able use a Collision Avoidance disabled UAV to strike departing or arriving aircraft, creating havoc for the passengers and crew, as well as bystanders and crew on the ground.

Additionally, there is widespread concern on the takeover of smart vehicles and aircraft. In the Wired article *Hackers Remotely Kill a Jeep on the Highway-With Me in It*, Andy Greenberg highlights the many issues we might see with the advent of intelligent and autonomous cars. In his article, Greenberg stated that it was possible for hackers to not only honk the horn and jerk the seat belt, but also take control of the steering wheel and disable the brakes (Greenberg, 2015). The hackers were able to remotely access the vehicle through a cellular network and issue commands like turning on the air conditioning and radio, as well as turn the engine off on the highway. The implications of exploits expressed in these scenarios speak for themselves. It is possible to do much more damage than shown here, especially by having control over steering systems and acceleration. In 2015, Chris Roberts, a computer security expert, told FBI agents that he had hacked into the in-flight entertainment system on multiple aircraft including B-737s, B-757s, and A-320s (Weise, 2015). In one of his attempts, he was capable of overriding the aircraft’s thrust management computer, forcing one of the engines to climb, causing the aircraft to fly sideways. This exemplifies the urgency in which we need to protect our CPSs. If cyber-terrorists had the knowledge and capability to control aircraft, there could be universal devastation.

With the rise of Cyber Kinetic attacks, the cybersecurity community is emphasizing our vulnerabilities and developing methods to protect our current and future infrastructure. The Department of Defense aims to inform and train cyber operators in Cyber Kinetic warfare to enhance armed engagements on the battlefield. In Rotem Guttmann’s article *Combined Arms Cyber-Kinetic Operator Training*, Guttmann shares part of the training received by these cyber warfare operators and proves the concept in a virtual environment. He states that cyber operators are able to support kinetic infiltration teams by gaining network access, killing the lights and disabling detection devices, obtaining enemy security camera feeds, preventing the alarm system from triggering, and more (Guttmann, 2017). Along with offensive training, it is also imperative for our cybersecurity experts to find ways to protect our technologies by staying informed with the latest exploit attempts, analyzing threats, and producing patches and upgrades that will defend against cyber attacks. Specifically, cybersecurity experts should focus their attention on the deadliest aspects of cyber threats we progressively face today, Cyber Physical Systems.

As technology progresses, new threats emerge daily.  The cyber domain is evolving, incorporating the physical domain, drastically increasing the significance in which we require protection. The capability to inflict physical harm without physical presence can be compared to telekinesis, the next step in warfare.  The ways in which cyber-terrorists work is uncanny and unpredictable; seemingly inspired by TV and film. We should learn from historical events and analyze the ideas and concepts being incorporated in an attempt to thwart future threats. If we wish to preserve our nation and our people, we must rise to meet advances in technology, and we must remain vigilant in our information age.

# Bibliography

Applegate, S. D. (2013). The Dawn of Kinetic Cyber. *2013 5th International Conference on Cyber Conflict (CYCON 2013)* (pp. 1-15). Tallinn, Estonia: NATO CCD COE. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6568376&isnumber=6568361

Behzadan, V. (2017). *Cyber-Physical Attacks on UAS Networks- Challenges and Open Research Problems.* Retrieved from https://arxiv.org/abs/1702.01251

Greenberg, A. (2015, July 21). Hackers Remotely Kill a Jeep on the Highway-With Me in It. *Wired*. Retrieved from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Guttmann, R. (2017, March 20). *Combined Arms Cyber-Kinetic Operator Training*. Retrieved January 13, 2018, from SEI Insights: https://insights.sei.cmu.edu/sei\_blog/2017/03/combined-arms-cyber-kinetic-operator-training.html

Ivezic, M. (2017). *Cyber-Kinetic Security.* Retrieved from http://ivezic.com/wp-content/uploads/2017/11/Cyber-Kinetic-Attacks-Chapter-2-The-History-of-Cyber-Kinetic-Attacks-and-Incidents.pdf

Kushner, D. (2013). *The Real Story of Stuxnet.* IEEE Spectrum. Retrieved from https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

O'Hara, B. (2015, November 18). *When a Cyber Attack Goes Kinetic*. Retrieved from SalientCRGT: http://www.salientcrgt.com/when-a-cyber-attack-goes-kinetic/

Weise, E. (2015, May 16). FBI: Computer Expert Briefly Made Plane Fly Sideways. *USA Today*. Retrieved from https://www.usatoday.com/story/tech/2015/05/16/chris-roberts-fbi-plane-hack-one-world-labs/27448335/

Yampolskiy, M., Skjellum, A., Kretzschmar, M., Overfelt, R. A., Sloan, K. R., & Yasinsac, A. (2016, September). Using 3D Printers as Weapons. *International Journal of Critical Infrastructure Protection, 14*, 58-71. doi:10.1016/j.ijcip.2015.12.004