2013 5th International Conference on Cyber Conflict
K. Podins, J. Stinissen, M. Maybaum (Eds.)

The Dawn of Kinetic Cyber

Scott D. Applegate
Center for Secure Information Systems
George Mason University
Fairfax, Virginia 22030
sapplega@gmu.edu

Abstract: Cyber attacks are often called non-violent or non-kinetic attacks, but the simple truth is that there is a credible capability to use cyber attacks to achieve kinetic effects. Kinetic Cyber refers to a class of cyber attacks that can cause direct or indirect physical damage, injury or death solely though the exploitation of vulnerable information systems and processes. Kinetic cyber attacks are a real and growing threat that is generally being ignored as unrealistic or alarmist. These types of attacks have been validated experimentally in the laboratory environment, they have been used operationally in the context of espionage and sabotage, and they have been used criminally in a number of attacks throughout the world. While these types of attacks have thus far been statistically insignificant, the rapid growth and integration of cyber physical systems into everything from automobiles to SCADA systems implies a significant kinetic cyber threat in the near future. It is imperative that the security community begin to take these types of threats seriously and address vulnerabilities associated with cyber physical systems and other devices that could be utilized to cause kinetic effects through cyber attacks.

Keywords: *kinetic cyber, cyber attacks, cyber conflict, cyber warfare*

1. INTRODUCTION

In the box office hit, *Live Free or Die Hard*, actor Bruce Willis takes on a group of cyber terrorists who begin systematically shutting down the United States by conducting cyber attacks and exploitation of critical infrastructure systems. In the midst of the movie, the main antagonist uses cyber attacks to inflict massive physical damage, injuries and death. While this kind of cyber inflicted mayhem currently remains in the realm of screenwriters and science fiction authors, the concept of inflicting physical damage, injury or death through *Kinetic Cyber* is no longer just a fictional construct of creative minds. Kinetic Cyber refers to a class of cyber attacks that can cause direct or indirect physical damage, injury or death solely though the exploitation of vulnerable information systems and processes. There have been a number of cyber attacks and laboratory experiments over the course of the last decade that foreshadow the dawn of kinetic cyber as the logical evolution of cyber warfare.

Kinetic cyber attacks are a real and growing threat that is generally being ignored as unrealistic or alarmist. Regardless of the views of the doubters and naysayers, there is a growing body of evidence that shows kinetic cyber to be a valid and growing threat. These types of attacks have been validated experimentally in the laboratory environment, they have been used operationally in the context of espionage and sabotage, and they have been used criminally in a number of attacks throughout the world. It is imperative that the security community begin to take these types of threats seriously and address vulnerabilities associated with cyber physical systems and other devices that could be utilized to cause kinetic effects through cyber attacks.

2. CYBER PHYSICAL SYSTEMS

Generally, the main targets for kinetic cyber attacks are cyber physical systems (CPS). CPS refers to the tight conjoining of and coordination between computational and physical resources. CPS is the integration of computer systems with physical processes and its applications have the potential to dwarf the information technology revolution of the last few decades [1]. “The economic and societal potential of such systems is vastly greater than what has been realized, and major investments are being made worldwide to develop the technology” [1]. CPS technologies are being integrated across a broad spectrum of industry sectors. These systems can be found in medical devices, traffic control and safety, advanced automotive systems, process control, energy conservation, environmental control, avionics, instrumentation, critical infrastructure control (electric power, water resources, and communications systems for example), distributed robotics, defense systems, manufacturing, and smart structures [1].

Unfortunately, like other information technologies, most were originally designed with little or no security, or security has been added after the fact. Many of these systems rely on the security-through-obscurity concept rather than building security into the design process. For example, of the 40 plus position papers presented at the National Science Foundation's Workshop on Cyber Physical Systems in 2006, only two actually focused on security aspects of CPS and these were more concerned with the networks that support these systems rather than the actual systems themselves [2], [3]. Furthermore, none of the presentations or working groups directly addressed the security requirements of these systems.

CPS technologies are designed to have kinetic effects. They are designed to monitor and control physical processes through the use of computers and information technology. To a hacker or to someone who thinks outside-the-box, the mere fact of their existence and their interconnection to cyberspace implies that they could be manipulated and used for purposes other than those they were intended for. That is exactly what is happening. Hackers and security researchers are exploring the limits of these technologies and, as will be shown below, manipulating them to cause kinetic cyber effects both in the laboratory and in the real-world.

3. VALIDATION OF KINETIC CYBER

Cyber attacks are often called non-violent or non-kinetic attacks, but the simple truth is that there is a credible capability to use cyber attacks to achieve kinetic effects. Kinetic cyber attacks have been around for at least a decade and the ability to conduct these types of attacks has been validated in the laboratory environment through experimentation; in the operational environment to sabotage physical devices; and in the wild by hackers, hacktivists and other malicious actors.

A. EXPERIMENTAL VALIDATION

Security researchers love to find new and interesting ways to manipulate technology and are very good at thinking outside-the-box. For example, during an experiment to see if they could hack the firmware on a laser printer, it occurred to security researchers Salvatore Stolfo and Ang Cui that they might be able to manipulate the printer in such a way as to start a fire [4]. While they were unable to accomplish this due to thermal safety switches built into the printer's hardware, the mere fact that they thought to attempt this feat is very demonstrative of the types of experiments that are happening in laboratories and research facilities throughout the world. Whether it is trying to see if you can use a printer to start a fire, or determining what systems on a modern automobile can be hacked and controlled remotely, simple curiosity often drives security researchers to see how they can exploit vulnerable

technology to do things it was never intended to do, often with very dangerous consequences.

1) Project Aurora

The Department of Homeland Security (DHS) conducted an experiment in 2007 in which security researchers hacked into a replica of a power plant's control system to see if they could shut down a large generator. The Experiment, dubbed Project Aurora, was conducted at the Department of Energy's Idaho laboratory and its dramatic results were released on video showing a generator spewing smoke and shaking itself to death over the course of about 30 seconds [5]. Researchers conducting the experiment changed the operating cycle of the generator which sent it out of control and resulted in catastrophic damage [5]. This type of attack could cause enormous damage if it were used to attack an actual operating electrical power plant. Beyond the immediate damage to the generator itself, the time and cost to replace these large, industrial turbines is immense and it could take months for a power plant to come back online if a successful attack resulted in this type of damage. Such an attack could have enormous economic consequences for the region served by a targeted power plant if it were successful. There has never been a publically acknowledged, successful cyber attack against a power plant, but the result of this experiment did alarm officials both in the energy sector and in government. The power industry has long been aware of the potential threat that cyber attacks might pose and has voluntarily adopted higher information security standards than most other sectors. Additionally, some vulnerabilities associated with this experiment have since been addressed according to Robert Jamison, then acting undersecretary of DHS's National Protection and Programs Directorate [5].

2) Hacking Medical Implants

In 2008, security researchers at the Harvard Medical School's Beth Israel Deaconess Medical Center in Boston, the University of Massachusetts Amherst and the University of Washington in Seattle raised alarms that implantable cardioverter defibrillators (ICD) or other medical implants could be vulnerable to hacking with devastating consequences [6]. These researchers cautioned that ICDs and pacemakers could be maliciously reprogrammed to fail "to shock a speeding heart or, conversely, jolts one that is beating normally" [6]. These devices could be remotely accessed using wireless technology and a laptop computer and most used only an unencrypted username and password to secure access. In many cases, the password was simply the device's serial number. These researchers also showed that you could easily intercept data wirelessly from these devices including the patient's name, date of birth, medical ID number, patient history, the name and phone number of the treating physician, the date of ICD implantation, the model, and the serial number of the ICD [7]. Researchers from this same study published

a series of recommended security measures to make implantable medical devices more secure, yet four years later, these devices were still demonstrably hackable [7], [8].

Security Researcher Barnaby Jack recently presented positive proof at the 2012 Breakpoint security conference that ICDs and pacemakers were still highly vulnerable to exploitation. Unlike the previous study, Jack actually demonstrated the ability to deliver a deadly 830-volt jolt to a pacemaker by logging into it remotely after hacking it [8].

> [Mr Jack] found the secret command doctors use to send a "raw packet" of data over the airwaves to find any cardioverter-defibrillator or pacemaker in range and have it respond with its model number and serial number. This information allows them to authenticate a medical device to receive telemetry data and perform commands or software updates [8].

A malicious actor could issue commands to an IDC to jolt the heart, as Mr Jack showed in his demonstration, or to not respond to a failing heart in an emergency. Worse, Mr Jack stated that "it would be possible to write a worm for one particular brand of pacemaker and defibrillator, then have it spread to other devices within range, from person to person" [8]. The only thing preventing these types of attacks, especially for a sophisticated actor such as a nation-state, is the will and motivation to do them. Mr Jack's research showed that medical implant technology is designed to be easily accessible, does not use encryption, is remotely accessible from a distance of up to 12 meters and can have life-threatening implications if abused.

3) CarShark

In 2010, security researchers from the University of Washington, Seattle and the University of California, San Diego conducted two studies on modern automobiles to see what systems could be hacked and exploited [9]. The research was conducted in three phases using bench testing, stationary vehicles and road tests to validate each attempted exploit. The study demonstrated "the ability to adversarially control a wide range of automotive functions and completely ignore driver input - including disabling the brakes, selectively braking individual wheels on demand, stopping the engine, and so on" [9]. To facilitate their experiment, the researchers wrote a custom tool designed to act as a bus analyzer and packet injector on Controllable Area Networks. This tool was called CarShark [9]. While the initial experiment was very successful and researchers were able to control dozens of functions in the car from locking and unlocking doors to disabling brakes at high speeds, the initial design of the experiment involved only direct physical access to the car. Researchers had to hook a laptop directly to the on-board diagnostics port in order to exploit the various automotive functions [9]. Researchers received so many questions on whether these

exploits could be accomplished remotely that they conducted a follow-on study to validate the ability to do just that.

In their follow-on study, researchers examined the potential attack surfaces of a modern automobile and determined that "remote exploitation is feasible via a broad range of attack vectors (including mechanics tools, CD players, Bluetooth and cellular radio)" [10]. They further showed that all of the exploits demonstrated in their initial study could be exploited by means of any of these attack vectors and "that wireless communications channels allowed long distance vehicle control, location tracking, in-cabin audio exfiltration and theft" [10]. There is little doubt that using the techniques demonstrated in these two studies it would be possible to seriously injure or kill the occupants of a vehicle. Turning off the headlights and disabling the brakes on a vehicle driving at highway speeds at night could easily result in a life threatening accident. The ability to do this remotely combined with the ability to set the malware to self-delete after an accident would make it very difficult for investigators to discover this type of attack, especially if they were not actually looking for it in the first place.

While there has been a great deal of work done by researchers in laboratory settings, the use of kinetic cyber is not limited solely to experimentation. Kinetic cyber attacks have been used by curious teenagers, hackers, criminals, and disgruntled employees in the real-world and many of these activities actually precede the more formal work done in labs.

B. REAL-WORLD VALIDATION

Activists, terrorists or criminals are always looking for new and innovative techniques to accomplish their goals and this is just as true in cyberspace as it is in the physical domain. There have been a number of criminal cyber attacks over the last decade that have directly resulted in kinetic effects. Many of these kinetic cyber attacks predate the experiments discussed above. The idea of causing physical damage using cyber attacks is not new; it has simply been relegated to obscurity as an outlier or an aberration. The incidents discussed below demonstrate that kinetic cyber capabilities do exist and are being used by hackers ranging from curious teenagers to disgruntled employees.

1) Maroochy Water Services, Queensland Australia

Starting in February of 2000, Vivek Boden, a 49 year old disgruntled utility worker, waged a three-month long hacking campaign against Maroochy Water Services and the Maroochy Shire Council in Queensland, Australia [11]. Boden was a former employee of Hunter Watertech, an Australian firm that installed supervisory

control and data acquisition (SCADA) systems and he had been a member of the team that had designed and implemented the SCADA systems for Maroochy Water Services. After leaving Hunter Watertech on poor terms, Boden had applied for and been denied a job by the Maroochy Shire Council. In an act of revenge for being denied the job, Boden began hacking the very SCADA systems he had helped install and released over 264,000 liters of raw sewage at a variety of locations over the course of the next three months [12]. This attack led to damage of the local environment and unhealthy conditions for the local residents. "Marine life died, the creek water turned black and the stench was unbearable for residents," said Janelle Bryant of the Australian Environmental Protection Agency [13]. Boden was eventually caught, charged, convicted and sentenced to two years in jail. Boden's series of attacks is one of the first to have caused physical damage solely through the use of information systems.

2) Los Angeles Traffic Management Center, Los Angeles, California

Over two days in late August 2006, striking traffic engineers from the Engineers and Architects Association picketed the Los Angeles City Hall demanding a better pay raise than the city was offering them over the next three years [14]. City officials, fearing that the striking workers would cause chaos with the city's traffic system, took steps to block access for the striking engineers. Two traffic engineers, Gabriel Murillo and Kartik Patel, managed to bypass this effort and hacked into the system causing gridlock at four key intersections in the city over the next several days [15]. Although access had been blocked for the striking engineers, access remained in place for top managers and one of the engineers was able to illicitly log into the system using one of his managers' credentials. Murillo and Patel then targeted four key intersections and extended the timing of red lights for the most congested approaches to these intersections causing traffic to come to a virtual standstill [16]. "Cars backed up at Los Angeles International Airport, at a key intersection in Studio City, at access onto the clogged Glendale Freeway and throughout the streets of Little Tokyo and the L.A. Civic Center area" [17]. Although there were no accidents attributed to this incident and therefore no physical damage or injuries, it is not a far stretch of the imagination to see that hacking into traffic control systems could easily result in kinetic effects. There is a large body of knowledge available on the Internet in regards to hacking traffic lights, and while this incident involved an insider threat, traffic lights and traffic management control systems are a popular target among hackers. Murillo and Patel were caught, charged with seven felonies between them and eventually sentenced to serve 240 hours of community service and fines amounting to $6000 dollars [17].

3) Tramways, Lodz, Poland

In January of 2008, a 14-year-old Polish teenager rewired a television remote control to interact with the wireless switch junctions on the Lodz city tram system. The teenager then used the remote control to reroute trams and essentially turned the tram system into his own personal train set [18]. The problem was discovered when a driver attempting to steer his vehicle to the right was involuntarily taken to the left. As a result the rear wagon of the train jumped the rails and collided with another passing tram. "The rear wagon then swung off the rails and crashed into another passing tram, hurling screaming passengers to the floor" [19]. The teen's actions caused the derailment of four vehicles and resulted in minor injuries to more than a dozen passengers. Lodz "transport employees were reported as saying that they knew immediately that someone outside their staff had caused the accident" [19]. This attack, although only done as a prank, is significant in that it was the first cyber attack to directly cause injuries.

C. OPERATIONAL VALIDATION

Kinetic cyber attacks have the potential to become very dangerous or even game-changing technologies in cyber warfare and other aspects of cyber conflict. The CPS that kinetic cyber generally targets are highly lucrative in terms of strategic value, and the ability to degrade, damage or destroy such systems represents a valuable weapon to a nation-state's arsenal. While only one such kinetic cyber attack is publically known to have been used at the present time, it would be dangerously short-sighted to believe that more such weapons are not currently in development. The Stuxnet attack against Iran in 2010 serves as operational example of the use of kinetic cyber-weapons and its success, however limited, has ushered in a new arms race among nation-state developing cyber warfare programs.

1) Stuxnet

In 2010, stories began to emerge in the media of a new worm that was described as the first cyber-weapon – a piece of targeted malware designed specifically to find and destroy specific physical devices. The Stuxnet worm was more complex than any previously discovered piece of malware. It contained four Windows zero-day exploits and was able to propagate itself through USB flash drives, network shares, a remote procedure call (RPC) vulnerability or a print spooler vulnerability [20]. Stuxnet was also the first piece of malware ever identified to include a programmable logic controller (PLC) root kit. Stuxnet spread itself via Microsoft Windows but appeared to target a specific PLC, the Siemens S7-300 system, and only if that PLC was attached to two specific types of variable-frequency drives which had to be spinning between 807 to 1210 Hz [20]. Once these and other specified conditions

had been met, the Stuxnet worm would periodically modify the frequency of the variable-frequency drives to 1410 Hz and then to 2 Hz and then to 1064 Hz while simultaneously masking these changes from attached monitoring systems [20].

The Stuxnet virus is known to have infected at least 120,000 Microsoft Windows systems worldwide, however, it is only known to have damaged systems in the Fuel Enrichment Plant in Natanz, Iran. This has led to popular speculation that the Stuxnet worm was designed to specifically target this facility. Although exact numbers have not been released by Iran, it is believed that Stuxnet damaged more than 1000 centrifuges used in Iran's nuclear fuel enrichment program [21]. While Stuxnet remains the only kinetic cyber-weapon that has thus far been seen in the wild, its discovery legitimizes the use of kinetic cyber in an operational context. The use of Stuxnet will have long-term implications in cyber warfare. As retired General Michael Hayden put it, "We have entered into a new phase of conflict in which we use a cyber-weapon to create physical destruction, and in this case, physical destruction in someone else's critical infrastructure" [22]. In essence, Stuxnet has opened Pandora's Box when it comes to the militarization of kinetic cyber technologies, and now that it is open, there is no going back. Nation-states around the world will look at this event as legitimizing the use of kinetic cyber in the international arena and will begin integrating these technologies into their own cyber warfare programs.

The above examples illustrate that kinetic cyber is a valid and credible threat. Security researchers are finding new ways to exploit vulnerable CPS to achieve kinetic effects beyond those intended by design. Hackers, cyber-criminals and hacktivists are actively exploring information systems with cyber physical connections and attempting to cause kinetic effects. This leads to the question of how these types of attacks may evolve in the future.

4. THE FUTURE OF KINETIC CYBER

Major investments, development and research are currently being conducted in the area of CPS and these types of systems are becoming more pervasive in industrialized states. The growth of CPS implies that the probability of seeing more kinetic cyber attacks targeting these types of systems is going to grow. Taking into account the types of attacks and research that has already occurred, it is not difficult to extrapolate the direction that kinetic cyber could take. The most dangerous avenue of growth would appear to be in the areas of SCADA, implantable medical devices, and automotive technologies although there are certainly other areas that are ripe for exploitation.

From the perspective of a nation-state, the ability to do serious damage to a rival state's critical infrastructure represents a strategic advantage. If an attack were able to successful damage a significant number of large electrical power plants in a manner similar to the Project Aurora experiment, the consequences could be economically destabilizing to the target state. Replacing the electrical generators in these types of plants can take months and cost millions of dollars per generator. In the meantime, the customers served by these plants would remain without power. Economist Scott Borg noted that if an attacker managed to knockout power to a third of the United States for a period of three months, the economy cost would be upwards of 700 billion dollars which is the economic equivalent of 40 to 50 large hurricanes hitting at the same time [5]. This type of attack would be economically devastating and would have significant long-term consequences. While it is unlikely that a state would engage in this type of large-scale attack outside the bounds of an openly declared war, it would also be short-sighted to assume that only states will have access to these types of attacks.

Looking at the subversion of implantable medical devices or automobile control systems, these technologies could easily be exploited to injure or kill individuals or even groups of people. Such a use of kinetic cyber could be employed for murder or assassination of key figures. What makes this approach particularly insidious is that investigators would probably not realize there was a cyber-component to these actions. Given the number of car accidents in a typical year, it is not beyond reason to assume that investigators would simply accept that a mechanical failure had caused a fatal accident rather that some form of cyber attack. This is especially true if the exploit leaves little or no residue of itself in the system after the fact. Since there have been no known incidents of cyber attacks causing car accidents, why would an investigator even suspect that this might be the case? The same is true of implantable medical devices. A recent article in Fire Engineering magazine points out that there is a possibility that arsonists may find a way in the near future to start fires using cyber attacks and that arson investigators would be highly unlikely to look for this as an underlying cause of a fire [23]. These types of incidents could be going on today and there is very little chance that they would be discovered.

The potential use of kinetic cyber by criminals or as a means of engaging in cyber warfare is only limited by the ability of hackers and researchers to approach these technologies from an unconventional and innovative direction. These systems already have the capability to produce physical effects; it is therefore possible to subvert their functionality to do new and potentially dangerous tasks. Given the pervasive nature of network technology and the convergence of networked systems with cyber physical devices, these types of attacks are going to become far more common in the near future and the security community needs to begin addressing this problem now.

5. ADDRESSING THE GROWING THREAT

One of the first steps that should be taken in addressing the threat of kinetic cyber is to begin hardening CPS since these systems are often the main target of this type of attack. Security in CPS has followed the same trend that has been seen throughout the information technology industry. CPS devices were originally designed with little or no security. As a credible threat has emerged against CPS devices, designers and security researchers have begun to look at better ways to protect these vital systems. In 2012, the National Institute of Standards and Technology (NIST) held their first workshop on Cyber Physical Systems Security in Gaithersburg, Maryland. This was a two-day event with presentations and working groups focusing on a variety of industry areas such as smart power grids, SCADA, implantable medical devices and modern automobiles.

During the course of the NIST conference, a number of consistent themes emerged across all sectors of CPS. First and foremost was the need to create digitally signed and trusted instruction sets for cyber physical devices. Currently most CPS devices will accept instruction sets from any source so long as they have the correct format and syntax. This leaves devices highly vulnerable to exploitation through man-in-the-middle attacks and attacks which leverage packet injection such as those used in the CarShark experiment. Another suggested avenue of research involves the development of intrusion detection systems and reputation management systems for specific types of SCADA infrastructure such as smart power grids [24]. These types of security systems are vital in an environment where not all data that is received by a CPS device can be trusted.

The above recommendations could be added to existing CPS technologies, however, that is not an ideal solution. Manufacturers and developers of these technologies must strive to build robust security into cyber physical devices throughout all stages of their development lifecycle. Security that is baked in throughout the systems development lifecycle is generally more effective than security that is bolted on after the fact. This is true for both the software that runs these systems, and the hardware platforms and devices that CPS run on. Developing hardware level security for CPS can act as a final safety barrier against compromise and exploitation [25]. Another important aspect of CPS that requires attention is sensor data. CPS devices base many of their functions on real-time feedback from sensors. Researchers should focus development efforts on specific controls to ensure sensor and monitor data is protected in terms of integrity and availability [26]. As demonstrated in the Stuxnet attack, the ability to corrupt sensor and monitor data can blind operators to a problem in the midst of an attack and allow greater damage to occur before a compromise is discovered.

Implantable medical devices (IMD) represent another growing segment of CPS technologies which, due to the very restrictive environment they operate in and the critical nature of their functions, will need very specialized security protocols. Restrictions on size, power consumption and processing power preclude many traditional security applications, but developers must take security into account when designing these devices. These devices are regulated in the United States by the Food and Drug Administration (FDA). While the FDA does do some testing to ensure IMDs perform in accordance with written specifications in a safe and effective manner, they do not do security testing of these devices in the context of information security and assurance. Inclusion of security and resilience testing in the testing guidelines for implantable medical devices should be a top priority for security researchers in the medical community [27]. Additionally, a review of authentication and access control protocols for IMDs should be conducted to ensure they balance adequate protection with the need for emergency access by medical personnel [27]. As noted in the study by Barnaby Jack, many of these devices currently have access controls that are trivial to bypass. One area that could assist in efforts to strengthen authentication and access control is the development of suitable encryption technologies. Development of appropriate cryptographic techniques that could be applied where necessary in the restricted operation environment of IMDs would make it much more difficult for a malicious actor to wirelessly eavesdrop and steal credentials for these devices. Security for IMDs will require a delicate balance between confidentiality and availability since too much security on these types of devices could hinder doctors in an emergency situation, endangering the patient's life. However, as Mr Jack showed in his experiment, a lack of proper security could be equally dangerous.

Moving beyond technical solutions, it is important for policy makers, standards bodies, and governments to create reasonable and effective regulatory schemes to address security requirements in CPS. These devices are used in many sectors considered to be critical infrastructure. Industry has traditionally been resistant to new regulations and that will probably be the case with the CPS industries as well. That having been said, industry has the opportunity to take the initiative and voluntarily establish industry standards for security of CPS [25]. Doing so can serve to stave off overly restrictive efforts by government regulators and will allow the industry to shape the standards as they move forward. In additional to new regulatory schemes, governments and international bodies need to begin addressing kinetic cyber through diplomatic and legal efforts. Honest and open dialogue is needed in the international community to codify the definition of kinetic cyber and to establish thresholds for when these types of activities qualify as a use of force. Thus far, the international community has mostly avoided addressing cyber warfare and cyber conflict under the laws of armed conflict; however, the growing threat

of kinetic cyber should spur new efforts to address these issues in a meaningful and thoughtful manner. It would be better to tackle this issue now, before a major kinetic cyber event happens, rather than trying to address the issue in the passion and turmoil that often follows such events.

These recommendations merely represent a good starting point for addressing the threat of kinetic cyber. There is a great deal of additional research that needs to be done to develop and implement technical solutions to address threats to CPS. In addition to technical solutions, policy makers, both domestically and in the international community, need to create common sense regulations for the CPS industry and begin to explore legal frameworks for codifying and addressing kinetic cyber.

6. CONCLUSIONS

Kinetic cyber is a real and growing threat. Numerous experiments have shown that it is possible to subvert CPS to cause damage, injury or even death under the right circumstances. Real-world incidents over the course of the last decade have validated this concept as curious hackers and disgruntled employees have exploited vulnerabilities in CPS devices to cause physical damage and injuries. Stuxnet has operationally validated this concept as well in its use of kinetic cyber attacks to damage more than a thousand centrifuges at the Natanz fuel enrichment facility in Iran.

Kinetic cyber mainly exploits vulnerabilities in CPS. Designers and manufacturers of these technologies need to incorporate better security controls into these systems beginning at the requirements and design stage of the systems development lifecycle and proceeding through the entire process to retirement. Beyond technical solutions, policy- and lawmakers should begin to address this issue through new industry standards and regulations. The international community must also act to codify cyber warfare and cyber conflict under international agreements and the laws of armed conflict. While many would discount the idea of kinetic cyber as unrealistic, the events that have occurred thus far represent the beginning of these tactics and foreshadow more dangerous attacks ahead. It is important to tackle the problem of kinetic cyber now, in its infancy, before development of these technologies leads to more serious and deadly outcomes.

REFERENCES

[1] E. A. Lee, “Cyber Physical Systems: Design Challenges,” 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), pp. 363–369, May 2008.

[2] D. Kazakos, “Position Paper : Robust Communications Networks with Imbedded Security,” in National Science Foundation on Cyber Physical Systems, 2006.

[3] J. C. (Steve) Liu, “Secure plug and play architectures for cyber-physical systems A Position paper for the NSF workshop on cyber-physical systems,” in National Science Foundation on Cyber Physical Systems, 2006.

[4] A. Cui, M. Costello, and S. J. Stolfo, “When Firmware Modifications Attack : A Case Study of Embedded Exploitation,” in 20th Annual Network & Distributed System Security Symposium, 2013.

[5] J. Meserve, “US Sources : Staged cyber attack reveals vulnerability in power grid,” Cable News Network, 26-Sep-2007. [Online]. Available: http://www.cnn.com/2007/US/09/26/power.at.risk/index.html. [Accessed: 30-Oct-2012].

[6] L. Greenemeier, “Heart-Stopper : Could Hackers Hit Pacemakers , Other Medical Implants?,” Scientific American, 14-Mar-2008.

[7] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, “Security and Privacy for Implantable Medical Devices,” IEEE Pervasive Computing, vol. 7, no. 1, pp. 30–39, Jan. 2008.

[8] B. Grubb, “Fatal risk at heart of lax security,” The Sydney Morning Herald, Sydney, Australia, 06-Nov-2012.

[9] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, “Experimental Security Analysis of a Modern Automobile,” in 2010 IEEE Symposium on Security and Privacy, 2010, pp. 447–462.

[10] S. Checkoway and D. McCoy, “Comprehensive experimental analyses of automotive attack surfaces,” in 20th USENIX Security Symposium, 2011.

[11] M. Crawford, “Utility hack led to security overhaul,” Computerworld, vol. 2006, pp. 1–2, 2006.

[12] M. Abrams and J. Weiss, “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia,” in NIST Industrial Process Control System Workshop, 2008.

[13] T. Smith, “Hacker jailed for revenge sewage attacks Job rejection caused a bit of a stink,” The Register, 31-Oct-2001.

[14] S. Hymon, “Engineers, Architects Strike Out on Picket Lines,” Los Angeles Times, Los Angeles, California, 11-Sep-2006.

[15] S. Bernstein and A. Blankstein, “Key signals targeted, officials say,” Los Angeles Times, Los Angeles, California, 09-Jan-2007.

[16] M. Krasnowski, “2 men accused of hacking into traffic system,” The San Diego Union-Tribune, San Diego, CA, 21-Jan-2007.

[17] S. Grad, “Engineers who hacked into L.A. traffic signal computer, jamming streets, sentenced,” Los Angeles Times, Los Angeles, California, 01-Dec-2009.

[18] J. Leyden, “Polish teen derails tram after hacking train network,” The Register, 11-Jan-2008.

[19] G. Baker, “Schoolboy hacks into city’s tram system,” The Telegraph, 11-Jan-2008.

[20] A. Matrosov, E. Rodionov, D. Harley, and J. Malcho, “Stuxnet under the microscope,” 2010.

[21] D. Albright, P. Brannan, and C. Walrond, “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant ?,” Washington D.C., 2010.

[22] A. Bloom, “60 Minutes - Stuxnet: Computer worm opens new era of warfare,” CBS News, 2012.

[23] K. Coleman, “Arson by Cyber Attack,” Fire Engineering, 12-Dec-2012. [Online]. Available: http://www.fireengineering.com/articles/2012/12/arson-by-cyber attack.html. [Accessed: 18-Dec-2012].

[24] R. Moreno, “Cyber-Physical Systems Security for the Smart Grid,” in Cybersecurity in Cyber-Physical Systems Workshop, 2012.

[25] A. Weimerskirch, “Safety-Critical Automotive and Industrial Data Security (Extended Abstract),” in Cybersecurity in Cyber-Physical Systems Workshop, 2012.

[26] M. Ben Salem, “Security Challenges and Requirements for Control Systems in the Semiconductor Manufacturing Sector (Extended Abstract),” in Cybersecurity in Cyber-Physical Systems Workshop, 2012, pp. 1–3.

[27] S. Gupta, “Implantable Medical Devices - Cyber Risks and Mitigation Approaches,” in Cybersecurity in Cyber-Physical Systems Workshop, 2012.