Chapter 2 Appendix: Timeline of Cyber-Kinetic Incidents and Research

Types of incidents

- Malfunction = Incident stemmed from an accidental malfunction within a cyber-physical system.
- Collateral damage = Incident stemmed from a virus or worm that did not specifically intend to cause kinetic impacts.
- Targeted attack = Incident is a confirmed or suspected targeted attack of cyber-physical systems with intended kinetic impacts.

Note: Targeted cyber-kinetic attacks are also bolded.

Year	*Incident*	*Type*	*Comments*
1982	**Explosion of Siberian natural gas pipeline**	**Targeted attack**	**Claimed by a former U.S. CIA operative to have been achieved by inserting malicious code into Canadian pipeline software that Soviet operatives were trying to steal.**
1985-1987	Therac-25 radiation poisoning	Malfunction	Six cancer patients died or suffered serious damage from malfunctions in radiation therapy equipment.

1996	Ariane 5 Rocket Explosion	Malfunction	The 1996 maiden launch of the Ariane 5 rocket by the European Space Agency ended spectacularly with a malfunction causing it to explode 40 seconds after lift-off. The cause was tracked to a single integer overflow coding error.
1997	U.S.S Yorktown stranded	Malfunction	A computerized U.S. Navy warship's propulsion system was disabled by bad data that it was not equipped to handle.
1997	Worcester Airport control tower lost communication	Collateral damage	A teen's hack of a Boston area telephone system cut off communications for the airport control tower and other critical systems.
1999	Bellingham, Washington, pipeline rupture	Malfunction	Poor programming practices led to a pressure buildup and subsequent explosion that killed three people, injured eight others and released a quarter-million gallon of gasoline.
2000	**Maroochy Shire wastewater**	**Targeted attack**	**A disgruntled contract worker released 264,000 liters of raw sewage around the**

	plant compromised		**township in revenge for not being offered a permanent position with the facility.**
2003	Davis-Besse nuclear power plant worm	Collateral damage	A worm entered the power plant's network through a T1 line between a contractor and the plant that the plant's staff didn't know existed. Critical systems were unavailable for five hours but, fortunately, the plant at that time was shut down for maintenance.
2003	Worm cripples CSX transport system	Collateral damage	A worm shut down rail and commuter transport for 12 hours on the U.S. East Coast.
2005	Worm cripples industrial plants	Collateral damage	A worm left workers idle at Daimer-Chrysler, Caterpillar and Boeing plants while IT staffs patched infected Windows systems.
2005	Taum Sauk dam failure	Malfunction	Discrepancies between pressure gauges at the dam and at the remote monitoring facility led to the release of a billion gallons of water, destroying 281 acres of state park land.
2006	Browns Ferry	Malfunction	Excessive traffic on ICS

	nuclear plant		systems caused two circulation pumps to fail.
2006	Harrisburg, Pennsylvania, water filtration plant hack	Collateral damage	A hacker gained control of sensitive systems but, fortunately, did not realize what he had gained control of. He used the network that controlled the systems merely to send spam emails.
2006	**Los Angeles traffic system attack**	**Targeted attack**	**Two city employees caused traffic lights to malfunction, snarling traffic, in an attempt to pressure the city to accept union bargaining demands.**
2008	Hatch nuclear power plant	Malfunction	Glitches in a software update provided erroneous readings of water levels that triggered a plant shutdown.
2008	**Lodz, Poland, tram hack**	**Targeted attack**	**A teen's hack of the tram system escalated to the point where a dozen passengers were injured, making this the first cyber-kinetic attack to result in human injury.**
2008	**Internet attack on epileptics**	**Targeted attack**	**A hacktivist group hacked the website of the Epilepsy Foundation and inserted graphics designed to trigger**

			migraines or seizures in epileptic patients
2008	Pacific Energy Resources hack	Targeted attack	A contractor compromised multiple systems and impaired operations in revenge for not being offered a permanent position. Fortunately, little damage was done.
2008	Turkish oil pipeline rupture	Targeted attack	Pipeline rupture cut off oil supplies to the nation of Georgia at a time when political tensions between Russia and Georgia were high, leading to suspicion of a Russian attack.
2009	Texas power company hack	Targeted attack	A fired employee hacked the system to cripple power forecasting systems, but could have used his access to inflict massive damage.
2009	Stuxnet attack on Iranian nuclear power facility	Targeted attack	A worm created by U.S. CIA and Israeli government targeting Iranian uranium enrichment devices destroyed as many as 10% of the illegally obtained and operated uranium enrichment

			centrifuges at an Iranian nuclear facility.
2010	San Bruno gas pipeline explosion	Malfunction	Erroneous readings led to a pressure overload that caused a rupture that killed eight, injured 60 and destroyed 37 homes.
2010	Marshall, Michigan crude oil spill	Malfunction	Multiple system malfunctions slowed response to the spill, leading to a discharge of 819,000 gallons of crude oil into the Kalamazoo River.
2011	**Houston, Texas, water distribution system hack**	**Targeted attack**	**A Romanian hacker shows evidence that he had easily breached the distribution facility. Fortunately, his motivation was only to embarrass officials who had publicly downplayed the seriousness of the Springfield water utility malfunction.**
2013-2016	**Unidentified nuclear power plant**	**Targeted attack**	**A top official of the International Atomic Energy Agency admitted that an unnamed nuclear power plant had suffered a cyber-kinetic attack sometime in that timeframe, but had managed**

			to defeat the attack without requiring a facility shutdown.
2014	**German steel mill attack**	**Targeted attack**	**Hackers inflicted massive damage on an unidentified German steel mill by disabling shutdown safeguards and operating equipment beyond their breaking points.**
2015	**"BlackEnergy" Ukrainian power grid attacks**	**Targeted attack**	**Russian government-sponsored hackers are believed to have disrupted Ukrainian power grids, leaving more than 80,000 people without power.**
2016	**Ransomware attacks on hospitals**	**Targeted attack**	**At least 19 hospitals suffered ransomware attacks in 2016.**
2016	**Unidentified water distribution facility attack**	**Targeted attack**	**A hacktivist group with ties to Syria gained control of critical systems of the facility, which has not been identified for security reasons. Had the hackers known how to use the system they had compromised, they could have inflicted mass casualties. Fortunately, they did not.**

2016	San Francisco transportation system ransomware attack	Targeted attack	Ransomware attack on municipal transportation system was quickly defeated, but evidence found in connection with the attack suggests that the perpetrator had successfully obtained ransom from a number of industrial victims.
2016	Lappeenranta, Finland, attack	Targeted attack	A hacker shut down heat and hot water in two apartment buildings.
2017	St. Louis, Missouri, library system ransomware attack	Targeted attack	Ransomware attack shut down St. Louis library system for two weeks while technicians rebuilt the computer system from scratch.
2017	Alpine ski resort ransomware attack	Targeted attack	Ransomware attack locks guests out of rooms and prevents the resort from creating new room keys.
2017	Unauthorized activation of Dallas, Texas, emergency sirens	Targeted attack	Emergency sirens sounded for more than 90 minutes in the middle of the night and system personnel had to shut down the entire system to stop them.

2017	**"WannaCry" ransomware attacks**	**Targeted attack**	**More than 75,000 hospitals, government agencies and businesses as large as Fedex and PetroChina in 99 countries found their systems locked and encrypted in a massive ransomware attack.**

Demonstrations of Vulnerabilities

Few key and first-of-the-kind researcher demonstrations:

Year	*Incident*	*Comments*
2007	Aurora Generator Test	Researchers demonstrated how power generators could be compromised and caused to explode by remote hackers.
2007	Tests of defibrillators and pacemakers	Researchers demonstrated vulnerabilities in defibrillators and pacemakers that could enable hackers to cause fatality to wearers.
2011	Tests of insulin pumps	Researchers Jerome Radcliffe and Barnaby Jack each demonstrated vulnerabilities that could allow hackers to administer fatal doses of insulin to diabetic patients.
2012	Researcher defeats key card locks	At the Black Hat security conference in Las Vegas developer Cody Brocious demonstrates a hack of key card locks that are in use in four million hotel rooms.

2014	Tests of traffic system vulnerabilities	Researcher Cesar Cerrudo demonstrated the ease with which sensors and control systems could be compromised with false data that could cause widespread system disruption.
2015	Test of smart rifles	Researchers Runa Sandvik and Michael Auger demonstrated a hack of a smart rifle that uses computer-aided aiming. Researchers managed to prevent the gun from firing, make it miss its target, and even tweak the targeting system so precisely that the bullet could hit a target of researcher's chosing rather than the original target.
2015-17	Researchers remotely take control of cars	Researchers Charlie Miller and Chris Valasek demonstrated vulnerabilities of computerized systems that control throttle, braking and steering of popular passenger vehicles. Chinese researchers demonstrated similar vulnerabilities, and my team has demonstrated the ability to remotely take partial control of multiple vehicles simultaneously.
2016-17	Researchers defeat geofencing safeguards on drones	My team has demonstrated vulnerabilities in drone geofencing safeguards that are meant to protect airports, military installations and major events.

2017	Tests show vulnerabilities of ICS systems	Security consultant Alexandru Ariciu demonstrated how ransomware attacks could target SCADA devices.
2017	Tests show vulnerabilities of industrial robots	Trend Micro researchers demonstrated multiple attack vectors in industrial robots that are vulnerable to attack by hackers.
2017	Tests show vulnerabilities of superyachts	Researcher Campbell Murray demonstrated the ease with which superyacht navigation, communication and Wi-Fi systems could be controlled remotely by hackers.
2017	Test demonstrates vulnerabilities of a commercial aircraft	Passenger jet controls hacked remotely while on the runway by a team of US government, industry and academic officials.