Cyber Can Kill and Destroy Too:
Blurring Borders Between Conventional and Cyber Warfare

Marina Krotofil, Institute for Security in Distributed Applications, Hamburg University of Technology, Hamburg, Germany

ABSTRACT

Cyberwarfare has become a fashionable topic in the last decade, partly because of the ever increasing sophistication of computer attacks, partly because of malicious actors setting their sight on industrial systems such as plants. Modern production systems are characterized by an IT-infrastructure controlling effects in the physical world. Such systems are called cyber-physical systems. In this paper the authors draw a distinction between information cyberattacks and cyber-physical attacks. Thereafter we provide insights into the specifics of cyber-physical attacks and examine to which extent they are similar to conventional warfare.

Keywords: Conventional Warfare, Cyber-Physical Attacks, Cyberwarfare, IT-Infrastructure, Modern Production Systems

DOI: 10.4018/ijcwt.2014070103

1. INTRODUCTION

The invention of computing machines and the subsequent creation of the Internet induced the emergence of a new space – digital space or cyberspace. Information technologies have quickly found their applications in all areas of life. They have also quickly become regular means of fraud and abuse. In the modern world there is a broad range of malicious actions in cyber space, ranging from abuses by script-kiddies to crime, espionage, attacks and political actions (hacktivism). Particularly damaging activities such as espionage and targeted attacks are often referred to as cyber warfare. Questions persist whether offensive cyber capabilities can be utilized for strategic and tactical war operations.

Technological change as a product of industrialization has transformed warfare from gunpowder to precision-guided munitions and stealth fight machines. The ability to create new technologies and transform them for martial benefits had been an essential part of military evolution. It is therefore not surprising that cyber means has also found their way into military affairs. Nevertheless the hostility, self-sufficiency of cyber weaponry and its particular role in conventional conflicts remains a topic of heated dispute (Leed, 2013; Libicki, 2013; Rid, 2013).

Discussions on cyber war mainly revolve around information and communications matters such as mass-harvesting of online communications, immense exfiltration of documentation, computer crime as well as disruption of the information and communications systems, including military and civilian command and control channels. It is therefore often contended that cyber activities cannot cause destructive causalities similar to conventional war. This assertion holds for data-targeting cyberattacks in the context of information cyber warfare.

Miniaturization of processors has enabled them to replace analog components in many electronic products. Further integration of microprocessors with input and output system components has evolved into microcontrollers. They became ubiquitous with applications ranging from consumer electronics to complex industrial systems. Many microcontrollers are part of purpose built computational systems embedded in applications in the physical world. Such collaborating environments consisting of computational and communication elements controlling physical entities with the help of sensors and actuators are called cyber-physical systems (CPS). On one hand embedded computers enable governing of physical applications to achieve desired outcomes. On the other hand, in the same way physical systems can be instructed to perform what is not intended. Thereby, software code which does not inherently possess tangible force acquires destructive capacity through the ability to instruct physical systems to malfunction. Cyberattacks on physical systems are correspondingly called cyber-physical attacks. The implications of this class of cyberattacks (the ability to inflict physical damage) can be compared to the kinetic impact of conventional weaponry. At that, malicious software can be seen as a warhead or as a detonator – one can choose.

At the current time the discussion about potential combativeness and actual feasibility of cyber-physical attacks is nevertheless largely premature as the world has not seen many full-fledged cyber-physical attacks yet. Advancing the state of knowledge about these questions, however, could and should be persevered. In the absence of a physical experimental infrastructure it can be pursued through ways that are relatively inexpensive, e.g. through modelling and simulations. For that purposes we adapted models of the realistic chemical plants Tennessee Eastman (TE) (Down, Vogel, 1993; Ricker, 2002) and Vinyl Acetate Monomer (Chen, et al., 2011; Luyben, Tyréus, 1998) to study physical processes exploitation and defence techniques. Some results of our research are included in this work.

The aim of this paper is twofold. Firstly, after drawing a distinction between information cyberattacks and cyber-physical attacks we give evidences that due to the ability of cyber-physical attacks to cause impacts beyond digital space the line between conventional and cyber ammunition is becoming very thin. Secondly, we provide insights into the specifics of cyber-physical attacks. In particular we dwell on a case of targeted cyber-physical attacks on process control systems such as a chemical plant or a refinery. We will show that general rules and attributes of conventional war are equally applicable to the cyber-physical assaults.

2. TERMINATORS IN CYBERSPACE

While there has been no publicly known murder committed by means of a computer-enabled attack yet, there have been public demonstrations that cyber-physical attacks can be launched to cause fatalities. At the same time, history has already witnessed examples of remote attacks causing physical damage.

Medical devices are meant to save lives. E.g., a pacemaker implanted in the chest sends regular electrical pulses to help maintaining a regular heart beat. Howbeit, these devices have little protection against unauthorized access via the wireless protocols used to access the widget. In a public video a researcher showed how he could remotely cause a pacemaker to suddenly deliver a lethal 830-volt shock from 50 feet (15.4 m) away (Kirk, 2012). In another presentation it was shown how insulin pumps from a particular vendor could be exploited wirelessly and made to deliver fatal doses of insulin to someone wearing the device (Radcliffe, 2011). Being aware of the medical devices remote exploitation danger Dick Cheney the former US Vice President had the wireless access to his pacemaker disabled (Gupta, 2013).

The most violent cyber attack to date is likely to have been Siberian pipeline explosion in 1982 in Russia. It was supposedly caused by CIA-initiated and covertly transferred hidden malfunctions in the Canadian automated control software. The malicious pipeline software was programmed to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds“ yielding most monumental non-nuclear explosion and fire ever seen from space” (Hoffman, 2004). However, according to Thomas Rid the available evidence on the event is so thin and questionable that it cannot be counted as a proven case (Rid, 2013). The laboratory attack on an electric generator is a proven case though; the machinery was caused to self-destruct by virtue of a remotely executed attack (Meserve, 2007). Stuxnet a tailored subversive malware which caused a number of centrifuges to fail physically (Langner, 2013) has certainly convinced many that advanced destructive abuses in cyber space are possible. While one may argue that the list of examples is too scant, the feasibility of the attacks should not be underestimated. Accident databases contain enough examples of both cyber-related and operations-related industrial incidents and disasters with human, machinery and environmental losses. Those scenarios might also be provoked intentionally. It would not be wrong to assume that national agencies are silently exploring the offensive potential of cyber-physical capabilities. It is also clear why the development of such arms is kept clandestine. Cyberattacks are single-use weapons. Every vulnerability disclosure and attack demonstration leads to fixes that make the next exploitation much harder.

Meanwhile the “Tallinn Manual on the International Law Applicable to Cyber Warfare” (Schmitt, 2013) which was written by 20 legal scholars and practitioners has captured the current reasoning on how current international law may apply to cyber war. In particular according to the authors, it is acceptable to retaliate against cyberattacks with traditional weapons if a state can prove that the attack lead to fatalities or to severe property damage. It is also stated that hackers who perpetrate attacks are legitimate targets for a kinetic counterstrike. In this regard the delimitation between cyber and conventional wars seems to loose its definition even further.

3. PROCESS CONTROL SYSTEMS AS THEATER OF WAR

Process control system (PCS) is an aggregated term for architectures, mechanisms and algorithms which enable processing of physical substances or manufacturing end products. Process industries include assembly lines, water treatment, pharmaceutical, food and other industries. Plants are strategic objects, especially those which are involved in military manufacturing, (petro)chemical production and utilities. The adversary might want to take control of them in order to disrupt production, break machinery or induce hazardous situations. Plants dealing with explosives, toxic and flammable chemicals and the like are thus subjected to risks of catastrophic accidents with lethal consequences for both plant personnel and members of the public. The Bhopal disaster in India in 1984 (Jung and Bloch, 2012) is one of the largest industrial accidents on record. A runaway reaction in a tank containing poisonous methyl isocyanate caused the pressure relief system to vent large amounts of chemicals into the atmosphere. The estimate of the death toll ranges from 4000 to 20000, with severe health problems persisting to the present.

In the past few decades plants have undergone tremendous modernization. Technology became an enabler of efficiency but also a source of problems. What used to be a panel of relays is now an embedded computer. What used to be a simple analog sensor is now an IP-enabled smart transmitter (Mclntyre, 2011) with multiple wired and wireless communication modes, numerous configuration possibilities, and even a web-server, so that maintenance staff can calibrate and setup the device without even approaching it. Thereby the possibility of remote exploitation of the physical processes and equipment became a reality. What is not always understood yet is that breaking into a system and taking over a device is not enough to carry out an attack. To actually break the system requires a different set of knowledge such as good understanding of mechanics, physics, chemistry and control principles.

Due to the multidisciplinary nature of plants it would require a team of technologists with highly specialised skills to design and conduct targeted large-scale attacks. Even if the cyber-warriors manage to break through all the IT-defences achieving the desired effects will be hampered by the plant operators' protective defences thus converting the plant floor into a battlefield. In the next sections we will show that strategies and tactics used in conventional military conflicts are the same as used for offence and defence in the industrial cyber-physical war game.

3.1. Espionage, Reconnaissance, Deception

As each facility is uniquely customized even operational sites within the same company can be very dissimilar. The same applies to systems failure modes. Therefore offensive capabilities in the cyber-physical domain exist only in relation to a specific target, which must be scoped to be understood.

The last few years were marked by the discovery of a large number of espionage campaigns and sophisticated spying malware directed at industry-related companies, e.g. (Chien and O'Gorman, 2011; Symantec Security Response, 2014; Kaspersky Global Research, 2014). The attackers are especially interested in user credentials and in intellectual property such as design documents, formulas, manufacturing processes, etc. While information on supporting IT and communication infrastructure is necessary for obtaining persistent access and gaining control, the data on processes, configurations and equipment is required to design actual cyber-physical attacks. Different equipment is susceptible to different classes of physical damage (Larsen, 2007). In addition carrying out an attack requires identification of process control system weaknesses and flaws which can be exploited.

Let us assume that the analysis of stolen information suggests that a chemical reactor relieve system is only designed to cope with the first exothermic reaction during normal operating conditions. This design weakness can be exploited by inducing a second exothermic reaction causing overpressure the relieve system would not be able to control. There are few approaches which may be applied for achieving the latter. One can manipulate the inflow or reactants, disable the cooling system or stop the mixer in the reactor. The decision on the strategy will depend on further weaknesses identified from the exfiltrated documentation, strategic considerations and/or personal preferences of the attackers (probably based on the expertise they possess). E.g., the root cause of the explosion at T2 Laboratories (4 killed, 28 insured) was a failed cooling system (CSB, 2009). The lack of cooling redundancy resulted in a runaway reaction. Because of insufficient relieve capabilities the pressure burst the reactor, the reactor content ignited and exploded. If the attacker is aware of both weaknesses, she only needs to disable the cooling system, which is subjected to a single point of failure, in order to achieve her goal.

As with many things in cyberspace a lot is simpler on paper than in reality. Hitting at outright success is difficult. The exact dynamic behavior of a process, precise mapping of I/O points, subtle correlation and interdependencies between components and physical phenomena are often not known even to the operators. The attacker can do her home work well and design most of the attack in advance; however she will have to tune the attack locally through reconnaissance activities such as changing configuration parameters or turning components on and off while observing the system's reaction. Getting the desired results also requires evading intrusion and anomaly detection guards so that those who administer the system cannot detect and eradicate the attack, and repair the damage quickly. Persisting within the target would therefore require reconnoitring the cyber assets, network design, security defences and safety countermeasures.

Military deception techniques aim to deliberately mislead adversary decision makers by luring them into taking specific actions or inactions. Deception can take different forms such as placing dummy and decoy equipment and devices or spreading false information on tactical actions or movement of forces. Similarly plant administrators may strategically place misleading or false technical documentation and use a simulated infrastructure to influence the attacker's target selection process and pilot her towards decoy physical processes as demonstrated in (Rrushi, 2011) for the example of a boiling water reactor. A particular case of deception in cyber space is the usage of honeypots – decoying vulnerable-looking cyber assets for studying attackers and their techniques. A recent report about a honeypot specifically developed to catch attacks against industrial control systems (Wilhoit, 2013) has demonstrated that the attackers not only have the skills to gain access to industrial systems but also posses knowledge on how to manipulate the equipment under control. The attacker may in turn use deception offensively. Among frequent causes of industrial accidents are missing alarms or wrong responses to abnormal events by the operators (ASM, 2013). The attacker may intentionally trigger certain alarms or cause alarm flooding to divert operator attention from the real problem or forcing her taking wrong actions.

3.2. Attack Strategies and Success Factors

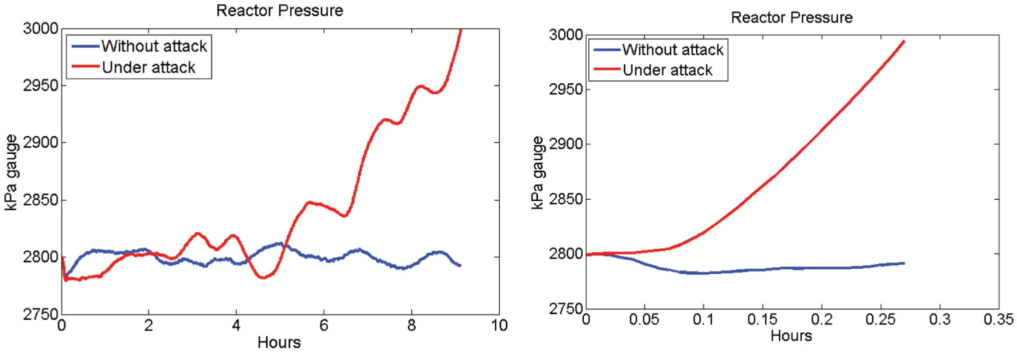
Conventional warfare is known as a strategic and tactic undertaking. Thorough planning and tailoring of activities to the situation at hand are necessary prerequisites for achieving success. Cyber-physical strikes are not different. The attacker might want to upset production, maximize physical damage, leave no traces, achieve results quickly, etc. Inducing specific unwanted effects requires playing radically different strategies specific to the process being attacked, but there are some general concepts that can be discussed. Foremost among those is time.

Misuse in IT the domain does not usually deal with time. A single bit flip can engage the burner under a tank of chemicals, but the reaction will still take hours to complete regardless of the state of the controller outputs. Changing the state of the outputs does not immediately put the process into a vulnerable state. An attacker needs to take into account the timing and state of the system and act when the process is in the vulnerable state. e.g., it may take minutes for a chemical reactor to burst (CSB, 2007), hours to heat a tank of water or burn out a motor, and days to destroy centrifuges (Langner, 2013). Understanding the timing parameters of the physical processes does not only allow an attacker to construct a successful attack but also to maximize its impact. In our previous work (Krotofil and Cárdenas, 2013) we have shown that the time it takes to bring a process to an undesired state depends greatly on a large number of parameters, among those the kind of relationships between the interdependent physical parameters and the way a physical phenomenon is being controlled, in particular, the configuration of the control loop which includes the choice of the manipulated variable (valve), type of the control algorithm and tuning parameters of a controller.

Figure 1 depicts TE process failure due to high reactor pressure brought on by data integrity attacks on different sensors. During such an attack the process measurements are forged to deceive controller about the currents state of the process and thus forcing it to take harmful compensating reactions. As can be seen the time to shutdown greatly differs. To obtain knowledge on such timing parameters the attacker would need to derive a behavioural process model of sufficient precision. This is a non-trivial task which is an active research area in process control engineering (Vodencarevic, et al., 2011).

Due to noise, disturbances, nonlinearity and instability of process behaviour the timing of the attack is another important strategic factor. Peak values (low and high) are usually of interest, in particular for launching resonance attacks, such as water hammers (Leishear, 2013). Water hammers are formed due

Figure 1. Data integrity attack on separator recycle flow sensor (left) and reactor Temperature sensor (right)

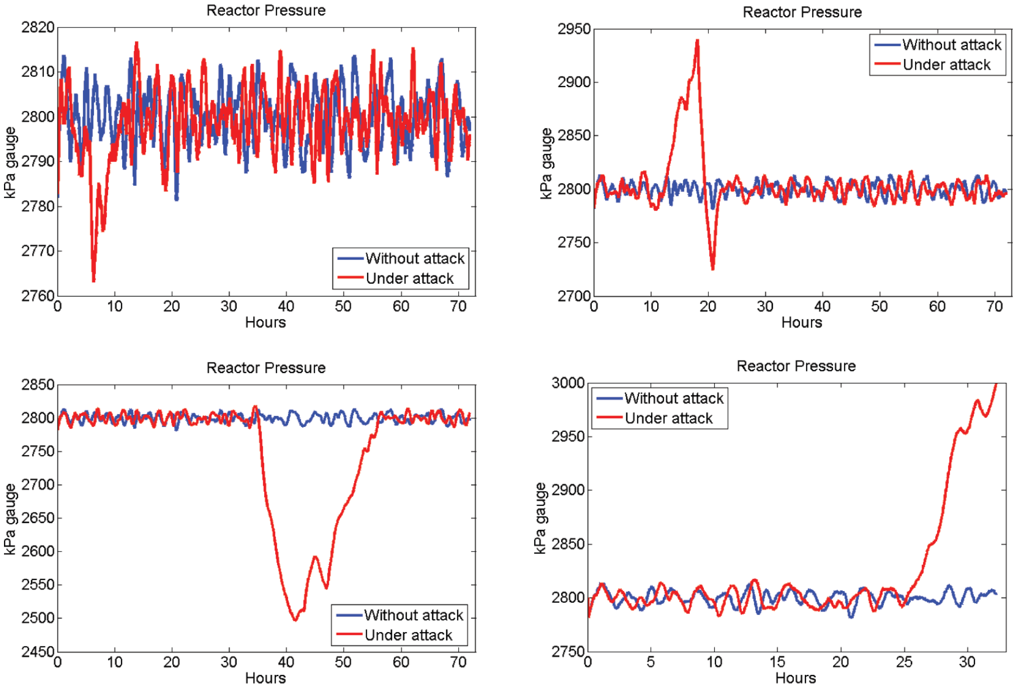


to waveform additions in fluids leading to a physical failure of the pipe.

In our experimental work we conducted an empirical study of the influence of *attack time* on the success of DoS attacks on sensor signals. DoS attacks on sensor-controller communication are effective in case the communication channel has integrity protections (e.g., message authentication codes) and the attacker does not have key material. DoS attacks on sensor signals prevents controller from receiving process measurements updates and make controller suing *stale data*. Usage of stale process measurements can drive the system to an unsafe state. Figure 2 demonstrates the outcome of a 10 hours long DoS attack on a reactor pressure sensor initiated at a random time. Depending on the time of attack the impact varies from negligible to a shutdown (experiment stopped before simulation time elapsed). If the attacker's goal is to induce an unsafe situation as soon as possible she would prefer to strike at attack at the time the process variable of interest reaches its local maximum or minimum (a more vulnerable state).

The next question to answer is how to decide on the best peak value to launch an attack as the sensor signal is relatively variable. The attacker faces the following problem: given a time series that exhibits a sequence of peaks and valleys of different amplitude, she has to select one of the peaks to launch a DoS attack in real time. If the attacker strikes too soon, she might lose the opportunity of having a higher impact on the system if she had waited longer (i.e., if the process variable would reach higher value later in the future). However, if the attacker waits for too long, the process variable might not reach a more vulnerable state than previously observed, and the adversary might miss the opportunity to cause maximal damage, or even have the implanted attack tools detected before they have the chance to launch the attack. The problem of selecting a good time to attack can be framed as an optimal stopping problem (Ferguson, 2006). These class of problems are concerned with the challenge of choosing the time to take a particular action based on sequentially observed random variables in order to maximize an expected payoff. Such class

Figure 2. Impact of 8h long DoS attacks on reactor pressure sensor at random time



of optimal stopping decision tasks in which the binary decision to either stop or continue the search depends only on relative ranks is modeled as Best Choice Problem, also known as the Secretary Problem (Freeman, 1983). In our recent work we evaluated different stopping algorithms to maximize the impact of stale data attacks (Krotofil, et. al., 2014). We showed that the problem the attacker has to solve is a non-trivial task in many practical situations as sensor measurements can be noisy and have sudden fluctuations. Moreover, certain types of sensor signals can make the selection problem even more challenging.

If the desired process upset is not instantaneous, plant operators may take corrective measures to bring the process back into its steady state. Moreover, if the operator attributes the process behaviour to unnatural causes, she can initiate an immediate incident investigation. Out of these considerations the attacker might prefer to hide the real process measurements from the operator. As a result, the operator loses situational awareness. This is one of the most dangerous attacks on process control. Besides changing the content of the operator's display, the adversary can spoof process data or play back pre-recorded normal operations measurements as implemented in the Stuxnet attack (Falliere, Murchu and Chien, 2010). A radically different approach would be to influence the process of taking measurement itself. This could be achieved through the manipulation of the surrounding environment or through miscalibration of the transmitters (sensors). Such an attack violates one crucial and predominantly overlooked security property of information called trustworthiness or veracity (Gollmann, 2012). E.g., in 2005 BP Texas City Refinery (CSB, 2007) suffered one of the worst industrial disasters in recent USA history. Explosions and fires killed 15 people and injured another 180. The root cause of the tragedy were critical alarms and control instrumentation providing false indications. Due to wrong calibration the splitter tower level indicator showed that the tower level was declining when it was actually overfilling with flammable liquid hydrocarbons. As a result the operator kept filling the tower. The further chain of events eventually led to an explosion.

3.3. Response

Despite of the full automation of most plants, human operators und maintenance personnel play a key role in process management and control, and are the main troops on the plant battlefield. During normal operating conditions operators are mostly responsible for the fine-tuning of control parameters to minimize the usage of raw materials, energy and efforts to produce best quality products. If process conditions are abnormal, the operator has the critical function of fault administration. Upon fault detection the problem has to be diagnosed and a decision has to be made on corrective measures. Sounds simple, but it is not.

Processes are generally highly complex and involve a high number of interacting variables and many degrees of freedom (valves). Variables can be cross-coupled, so that changes in one variable affect several other variables simultaneously. Modern control rooms comprise multiple displays with large number of controls and alarms to display these processes. In critical situations such complexity can severely overburden the operator and make it extremely difficult for her to identify the state of the plant. Furthermore, the decision-making process is predominantly based on experiences and training. Every previously unseen disturbance poses a significant mental challenge for the personnel. E.g., if the operator had never had to deal with water hammers before, she would likely not to be able to figure out easily how to resolve it (e.g. open the valve). Withal, the process variables and system responses can be slow and a control action may not produce a visible system response for seconds or minutes. As a result, stress and fatigue are intrinsic attributes of this job (Mannan, 2005).

Despite of the challenges outlined operators are largely capable of dealing with accidental process perturbations without initiating unit shutdown. However, during a coordinated attack events are not happening on the basis of statistical independencies and normal process flows. Hence there is a significant danger of operators taking wrong actions. Moreover the intruder might have endeavoured to estimate the operators' responses and develop strategies to withstand the defender's corrective actions. Hence gaining the upper hand can be difficult. Therefore it is crucial to be able to locate and isolate the source of an attack. This would first and foremost require collaborative activities with IT and security personnel as cyberattacks may leave traces in system logs and traffic dumps. Modern plants may also take advantage of Asset Management Systems which keep detailed diagnostic and maintenance-related information about field instrumentation to detect unauthorized manipulations.

Detection of compromised nodes requires conducting forensic activities. Uncovering controllers compromised by the authorized engineering station might be challenging due to the absence of anomalous activity logs. Since in cyber-physical systems the major evidences of misuse are in the physical world, it might be possible to trace perturbations back to the compromised end points. It is therefore desired to keep a process running to facilitate the attribution of the sources of the problems. In one of our ongoing works we design various cyber-attacks aimed at decreasing catalyst activity. Catalysts promote chemical reactions or accelerate the rate at which a chemical reaction approaches equilibrium. Catalyst activity is an attractive attack target as catalyst performance largely determines overall unit manufacturing costs. Kinetics of the catalyst decay is very complex and the reasons of the catalyst deactivations are not obvious at first glance (Birtill, 2003). It would require a multi-disciplinary process engineering team, detailed knowledge of process conditions and feedstock, time and patience to interpret behavior of catalyst deactivation and accurately determine the source of problems. The task of the operators during the investigation include achieving maximum possible production capacity while minimizing environmental impact caused by increased by-products waste and emissions (due to lower catalyst activity).

3.4. Defenses

To mitigate the threats one has to develop defenses. Any pilot knows when flying blind one has to trust the instruments. Fault diagnosis fully depends on the instrument readings. Hence it is important for the operator to have confidence that the measurements are correct. Preserving situational awareness is thereupon the cornerstone in PCS defence. This could be achieved through taking orthogonal measurements, performing plausibility and data consistency checks, calculating estimates, etc. What is important, implementation of such defences does not require physical changes in plant configuration and thus can be brought into practical service.

One of the most eminent similarities between military operations and cyber-physical systems is exposure to hazards and – consequently – requirement for safety measures. Process control history has accumulated substantial experience in identifying and addressing potential hazards and operational problems in terms of plant design and human error to minimise the effects of atypical situations and achieve a safe outcome from a situation that could have resulted in a major accident. However such analysis only considers natural causes of events and unintentional human mistakes within the organization. Communication technologies have in contrast introduced security issues such as external threats. The distinctive feature of intended abuses is the impossibility of predicting them (where, when and how). As a result it is difficult to asses whether system design will remain flaw-less and safety measures suffice if confronted with cyber-physical assaults. Conducting process-aware security risk assessment will help to identify PCS weaknesses in the presence of cyberattacks. While prioritizing equipment and systems which require most protection would require a list of hypothesized attack and evaluation of their probabilities, some steps of a security assessment such as the discovery of the latent abilities of the components can be conducted without having a particular misuse case in mind. Thus most of the equipment is manufactured for more than one purpose. E.g., a motor that can be run in reverse but never used that way should have that option disabled.

Similarly to tactical military operations Industrial Control Systems are becoming increasingly dependent on critical information systems. In the military domain it was already recognized that the success of cyber security measures should be not be determined by the level of protection of critical network infrastructure components (routers, servers, etc.) and software assets (operating systems, data resources, application programs, etc.) from attackers but by the level of attainment of ongoing and planned mission objectives (Jakobson, 2013). The main goal of both PCS and the military is to achieve their operational goals (missions) in hostile and malicious operating environments. Therefore moving from IT-centricity towards architecting cyber-attack resilient missions will open PCS new opportunities in achieving the completion of operational goals even if the IT assets and services that are supporting the missions are under cyber-attacks. First works on the feasibility to evaluate the impact of cyber incidents on the physical domain has shown promising results (Barreto, Costa, Yano, 2012). Another military-style strategy called “kill-chain analysis” is recently adopted by the industry to swart advanced persistent threats (Hutchins, Cloppert, Amin, 2011). To achieve her malicious objective an adversary must complete a sequence of actions, commonly referred to as a “kill chain”. Because each step must work, the defenses can focus on assuring only on certain attack executions steps to make them impossible to achieve by the attacker.

Military exercises serve the purpose of studying warfare and training available skills and techniques in simulated scenarios. Similarly cyber-security drills strengthen readiness to accidental and targeted attacks and bolster defences. Such an exercise simulates what would happen if the assailant penetrates certain systems and carries out a specific attack. Since in CPS the attacker ferrets her way to the physical world through the cyber layer it is crucial to conduct collaborative trainings including both IT and process control divisions. Such joint exercises will enable these usually disjoint groups to practice sharing information with each other, learn making real-time critical decisions for mitigating threats and conduct coordinated forensic activities. Also, the process control group should include multidisciplinary participants to train diverse attack detection (e.g., plausibility checks) and response techniques (e.g., dynamic controllability).

4. DISCUSSION

In the modern Information Age information has become a valuable asset. This being the case, information warfare has become an attractive domain for most small countries and developing nations because the amount of resources and effort that a country must invest to launch a cyberattack is significantly lower than fielding tanks, launching satellites, developing a secret agency or refining uranium (as is the visibility of such preparations). Besides, cyberattacks can be launched across borders. The advanced nation-states have therefore no longer a monopoly on war. Moreover, minor actors such as organized crime groups, insurgents and terrorist can also engage independently or at the behest of nation-states.

While acquisition of cyber capabilities is easy and tools are cheap, the cost of large-scale cyberattacks should not be underestimated. Even more resources are required to prepare a targeted attack on a complex cyber-physical target such as a plant. It would require lengthy coordinated preparatory work and a multi-skilled team with advanced competences. Thus, feasibility testing and tuning of the devised physical attack requires experimental labs with specialized industrial equipment similar to the one installed at the target site. Implementation and carrying out of an attack further (optionally but very likely) depends upon sophisticated and time-consuming firmware reverse engineering, root-kitting of embedded systems and discovery of 0-days vulnerabilities. Therefore the ability to design and conduct a full-fledged cyber-physical attack is likely to be beyond the capacities of individual groups and countries without sufficient resources. As follows, cyber-physical weaponry is likely to remain a privilege of developed countries or well-financed nations which can draw in mercenaries.

Concerning conventional war, certain countries have cut military expenditures out of economic considerations and accept the risk of being conquered. Similarly the defence capacity of plants might be consciously kept weak if addressing security concerns is not deemed justifiable. E.g., it was shown that the optimal operating condition for reactor pressure in the TE process is close to the upper shutdown limit of 3000kPa. In this case the attacker will be able to bring the system into an unsafe state quickly. To ensure secure operations it would be desirable to maintain a sufficient safety margin. However, maintaining a safety margin of at least 100 kPa is equivalent to a 5% increase in cost. Ease of maintenance and plant administration also clashes with security concerns. Usage of standard configurations and operating procedures, utilization of equipment and instrumentation of a single preferred vendor makes vulnerabilities predictable but is convenient for managing the plant.

Particularly dangerous is the homogeneity of field instrumentation firmware. In this case the attacker would need to discover vulnerabilities just once to invade multiple devices. An advanced attacker may further co-opt compromised devices into a botnet.

As can be seen from this short review paper, cyber-physical attacks, despite of carrying cyber component in them, are much closer to the essence of conventional warfare than to information cyber-attacks. However by all means more practice-oriented research is needed to determine further aspects of cyber-physical assaults.

REFERENCES

Abnormal Situation Management (ASM) Consortium. [online] Available at: https://www.asmconsortium.net [Accessed June, 2013].

Barreto, A. B., Costa, P., & Yano, E. A. (2012) Semantic Approach to Evaluate the Impact of Cyber Actions to the Physical Domain. *In Proceedings of 7th International Conference on Semantic Technologies for Intelligence, Defense, and Security* (pp. 64-71).

Birtill, J. J. (2003). But will it last until the shutdown? Deciphering catalyst decay! *Catalysis Today*, *81*(4), 531–545. doi:10.1016/S0920-5861(03)00152-4

Chen, R., Dave, K., McAvoy, T. J., & Luyben, M. (2003). A Nonlinear Dynamic Model of a Vinyl Acetate Process. *Industrial & Engineering Chemistry Research*, *42*(20), 4478–4487. doi:10.1021/ie020859k

Chien, E., & O'Gorman, G. (2011). *The nitro attacks: Stealing secrets from the chemical industry*. Symantec, Technical report.

Downs, J. J., & Vogel, E. F. (1993). A plant-wide industrial process control problem. *Computers & Chemical Engineering*, *17*(3), 245–255. doi:10.1016/0098-1354(93)80018-I

Falliere, N., Murchu L. O., & Chien, E. (2010). *W32.Stuxnet dossier*. Symantec, Technical report.

Ferguson, T. S. (2006) *Optimal Stopping and Applications*. [online] Available at: http://www.math.ucla.edu/~tom/Stopping/Contents.html [Accessed November, 2014]

Freeman, P. R. (1983). *The secretary problem and its extensions: A review* (pp. 189–206). International Statistical Review/Revue Internationale de Statistique.

Gollmann, D. (2012) Veracity Plausibility, and Reputation. In Information Security Theory and Practice, LNCS 7322, pages 20-28.

Gupta, S. (2013) Dick Cheney's heart. *CBSNews*, [online] Available at: http://www.cbsnews.com/news/dick-cheneys-heart/ [Accessed October, 2013]

Hoffman, E. D. (2004) CIA slipped bugs to Soviets. *The Washington Post*, [pdf] Available at: http://industrialdefender.com/general_downloads/incidents/1982.06_trans_siberian_gas_pipeline_explosion.pdf [Accessed October, 2013]

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011) Intelligence-Driven Computer Network Defence Informed by Analysis of Adversary Campaign und Intrusion Kills Chains. *In proceedings of the 6th Annual International Conference on Information Warfare*, pages 113-125.

Jakobson, G. (2013) Mission-centricity in cyber security: Architecting cyber attack resilient missions. *In proceedings of 5th International Conference on Cyber Conflict*, pages 1-18.

Jung, B., & Bloch, K. (2012) The Bhopal disaster. *Hydrocarbon Processing*, [online] Available at: http://www.hydrocarbonprocessing.com/Article/3035763/The-Bhopal-disaster.html [Accessed October, 2013]

Kaspersky Global Research. (2014). *Energetic Bear — Crouching Yet*i. Kaspersky Lab: Technical report.

Kirk, J. (2012) Pacemaker hack can deliver deadly 830-volt jolt. *Computerworld*, [online] Available at: http://www.computerworld.com/s/article/9232477/Pacemaker_hack_can_deliver_deadly_830_volt_jolt [Accessed October, 2013]

Krotofil, M., Alvaro, A., Cárdenas, A. A., Manning, B., & Larsen, J. (2014) CPS: Driving Cyber-Physical Systems to Unsafe Operating conditions by Timing DoS Attacks on Sensor Signals. In *Proceedings of the 30th Annual Computer Security Applications Conference*, pages 146-155. doi:10.1145/2664243.2664290

Krotofil, M., & Cardenas, A. (2013) Resilience of Process Control Systems to Cyber-Physical Attacks. In Secure IT Systems, LNCS 8208, pages 166-182. doi:10.1007/978-3-642-41488-6_12

Langner, R. (2013) To kill a centrifuge, [pdf] Available at:http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf [Accessed October, 2013]

Larsen, J. (2007) *Breakage.* [pdf] Black Hat USA. Available at: http://www.blackhat.com/presentations/bh-dc-08/Larsen/Presentation/bh-dc-08-larsen.pdf [Accessed October, 2013]

Leed, M. (2013) *Offensive Cyber Capabilities at the Operational Level* [pdf] CSIS. Available at: http://csis.org/files/publication/130916_Leed_Offensive-CyberCapabilities_Web.pdf [Accessed September, 2013]

Leishear, R. A. C. (2013). *Fluid Mechanics, Water Hammer, Dynamic Stresses and Piping Design*. ASME Intl. doi:10.1115/1.859964

Libicki, M. C. (2013) *Brandishing Cyberattack Capabilities* [pdf] RAND Corporation. Available at: http://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR175/RAND_RR175.pdf [Accessed September, 2013]

Luyben, M. L., & Tyréus, B. D. (1998). An industrial design/control study for the vinyl acetate monomer process. *Computers & Chemical Engineering*, *22*(7-8), 867–877. doi:10.1016/S0098-1354(98)00030-1

Mannan, S. (2005). *Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control* (Vol. 1). Butterworth Heinemann.

McIntyre, C. (2011) Using Smart Instrumentation. *Plant Engineering*, [online] Available at: http://www.plantengineering.com/home/single-article/using-smart-instrumentation/a0ec350155bb86c8f65377ba66e59df8.html [Accessed October, 2013]

Meserve, J. (2007) Staged cyberattack reveals vulnerability in power grid. *CNN*, [online] Available at: http://edition.cnn.com/2007/US/09/26/power.at.risk/ [Accessed October, 2013]

Radcliffe, J. (2011) *Hacking Medical Devices for Fun and Insulin.* [pdf] Black Hat USA. Available at: http://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_Slides.pdf [Accessed October, 2013]

Ricker, N. L. (2002) Tennessee Eastman Challenge Archive. Available at: http://depts.washington.edu/control/LARRY/TE/download.html [Accessed June, 2013].

Rid, T. (2013) *Cyber War Will Not Take Place.* Hurst & Co.

Rrushi, J. (2011). An exploration of defensive deception in industrial communication networks. *International Journal of Critical Infrastructure Protection*, *4*(3), 66–75. doi:10.1016/j.ijcip.2011.06.002

Schmitt, M. N. (2013). *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. doi:10.1017/CBO9781139169288

Symantec Security Response. (2014). *Dragonfly: Cyberespionage Attacks Energy Suppliers*. Symantec: Technical report.

U.S. Chemical Safety Board (CSB). (2007). *BP America Refinery Explosion: final investigation report.*

U.S. Chemical Safety Board (CSB). (2009). *T2 Laboratories Inc. Reactive Chemical Explosion: final investigation report.*

Vodencarevic, A., Kleine Buning, H., Niggemann, O., & Maier, O. (2011) Identifying behaviour models for process plants. In Emerging Technologies Factory Automation, pages 1-8.

Wilhoit, K. (2013) *Who is Really Attacking Your ICS Equipment*? Trend Micro Incorporated: Research Paper.