March - April 2020
ISSN: 0193-4120 Page No. 931 - 937

Critical Evidence on the Implementation of SCADA in the UAE: Artificial Intelligence Mandate Vulnerability, and Public Safety – Part 1

Omar Abdul Rahman Al Attas
Alhashemi Abu Dhabi Police UAE

Article Info
Volume 83
Page Number: 931 - 937
Publication Issue:
March - April 2020

Article History
Article Received*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 13 March 2020*

Abstract
The dependence of structural physical systems including Supervisory Control and Data Acquisition (SCADA) systems on AI technology is growing rapidly. The mandate of AI to achieve efficient and effective industrial supervisory systems is clear; however, threats resulting from both internal malfunctions and external cyber sabotage have become of crucial concern to SCADA systems that depend on AI. AI defence mechanisms are often installed within system architecture and through other external sources. Careful balancing of defence mechanisms to counter attacks and overcome systems vulnerabilities remain critical to the very protection of public lives which have become progressively reliant on these physical systems. In these developments, the passive role of human governance of technology systems cannot be wholly exempted. This paper employe the action research strategy with primary focus on two SCADA control rooms in the Emirate of Abu Dhabi. These control rooms handle over 60% of all non-law enforcement physical and infrastructural systems monitoring across the Emirate of Abu Dhabi. Operational AI integrated SCADA Systems are diagnosed with the help of document analysis and informal interviews. Action planning entails careful matrix modelling of possible courses of actions that balances AI defence and attacks in the SCADA environment. The implementation, evaluation, and specification of learnings are reserved for the second part of the present paper. The results of the first two stages of the action research are critically discussed to reveal evidence on how AI is operationalized in SCADA monitoring, data collection, and control centring.

Index Terms*—SCADA, public safety, Artificial intelligence, cybersabotage, cyber defence*

I. INTRODUCTION *(HEADING 1)*

Governments put their citizens first in all matters of national security, and public safety has been considered the basis for the prosperity and continuity of global socio-economic systems [1]. However, public safety remains complex with a vast number of interactive systems covering potential risks to both human and infrastructure [1] to social risks, the risk from technological developments (technical risk) and other natural risks [2][3][4]. Due to the complexity of public safety management systems, dependencies, tasks and environmental adaptations, it is not new that researchers have resorted to the complexity theory to permit systemic interpretation and evaluation modelling of public safety systems [4].

The overly complicated scope of public safety management systems accounts in part for the adoption of e-governance systems and Smart Cities to ensure efficient sharing of information, delivery of public service, and effective public sector governance [4][5]. In these related developments, the Supervisory Control and Data Acquisition (SCADA) Systems is one aspect Smart Cities with a high presence in industrial systems automation within an increasingly digitised public service delivery[5][6]).According to Ref [5]:

> *"SCADA system is a computer-based process control system used by a nation's infrastructure utility systems, that permits control and monitoring gathering field data from sensors and instruments located at remote sites, transmitting and displaying these data at a central site, and enabling engineers to send control commands to the field instruments".*

These systems help control industrial machinery in charge of water supply, electric power generation and distribution, mass transportation, and oil and gas production and distribution systems [5]. Control commands are sent to field instruments through information communication technology (ICT), usually web-based systems that operate over the internet [5]. Using these systems, a technician can control the traffic signals, water and gas pumps among other industrial valves from a distant location. With growing significance in today's national economies, the global SCADA market is estimated to reach 40.18 billion United States Dollars by 2024 [7].

Artificial intelligence (AI) and robotic process automation (RPA) have helped expand the functionalities

of SCADA systems to improve their overall capabilities [8]. This leads to what Ref [9] terms "intelligent SCADA systems". Industrial systems are becoming larger and complex, and AI is considered the best tool to conduct supervisor and control tasks efficiently and effectively by learning patterns, recognising anomalies and mimicking human response to events with little to no interference. By incorporating AI and RPA expert systems with high operational capabilities, industrial plants are able to make up for personnel shortage, identify flaws, fix these flaws, manage information overload and manage plant interface, all in a combined interrelated attempt through would easily elude humans.

As AI gains relevance in utilities, transportation, oil & gas and other critical infrastructure, threats targeted at AI renders these sectors vulnerable, and public safety is threatened [6][7]. Several global incidents are evidence of the threat to SCADA systems with detrimental effects on humans and infrastructure using AI-based attacks [10]. External AI threat level corresponds with the degree of unauthorised access. Most critical to external threat is the access points which depicts the time and duration where the client of the industrial system offers the SCADA operations room grant access to undertake emergency corrective measures [9]. Access to SCADA control room access point or portal holds the possibility of the highest amount of damage attackers can cause to any SCADA system. As such, deciding how much control to allocate to the AI over the SCADA is critical, since this may help save lives or offer attackers an opportunity to create maximum damage.

In the quest to understand how AI is operationalized amid existing threats and defences, evaluation models have focused categorically on one or a narrow aspect of security analysis, attack simulation, preventive systems, or post-damage evaluation [11][12][13][14][15]. These evaluation models are predominantly fragmented and tackle the individual elements of the cybersecurity environment. Very little has been done to capture AI threat and operational capabilities in a manner that captures embedded risks and benefits of the technology systems. This paper aims to propose an evaluation model for the analysis of AI-based SCADA systems that map attack against defence mechanisms to ensure public safety.

II. UAE Smart Government Agenda and Increased Adoption of AI by the UAE Government

In the UAE, the government is committed to the installation of smart government system for key operations [16]. This effort is to ensure that the entire government operating systems is intelligent-based and automated for optimum efficiency. Currently, a number of AI systems run key utility SCADA systems in the areas of electricity and water supply and transportation systems. SCADA has also become rather popular in oil and gas facilities, and the government aspires to expand into other sectors to reduce cost and improve overall government efficiency [17]. Ultimately, the scope of AI application is poised to increase, making more government infrastructural systems free from human intervention.

In related developments, the government believes that the backbone of business growth and effective service delivery is AI. The UAE Strategy for Artificial intelligence launched in 2017 is the first of its kind within the region, with key objectives integral to the UAE Centennial 2071 [18]. Through this strategy, the government aspires to improve performance at all government levels and make the UAE a leader in the field of AI investment by creating markets with high economic value. The strategy mainly covers the application of AI to key sectors including the transportation, healthcare, space, renewable energy, water, technology, education, environment and traffic sectors.

The UAE has made some important strides in cybersecurity and the development of developing integrated solutions for SCADA systems. Cassidian is one of the first technology companies to develop the SCADA protection solution that protects industrial control systems (ICS) from outside attacks for the UAE [19]. This solution, named Cymerius, ensures that SCADA systems are able to continue operations even in times of business interruptions including disasters. The system monitors both ICS and Business IT, with integration into a designed smartphone application. The AI integration permits encryption of phone calls and other interactions between business and SCADA control room operators to secure all access points [19].

In another application of AI to SCADA systems, the UAE plays an integral role in securing high level professional cyber defence services to audit security infrastructure architectures and implement control and operational centres with dedicated security supervision in SCADA and other technology systems [20]. Careful vulnerability and security assessment are conducted in all critical infrastructure and government facilities at various levels of violence whilst keeping in mind equal possibility of terrorism. Entities include public businesses in economic sensitive areas such as ADNOC, airports, seaports, water and power utilities, the nuclear plants being developed, energy sector, other oil and gas facilities among others [20].

As the role of AI in government and SCADA increases, such developments bring about new security challenges that require constant supervision to ensure that pertinent threats are mitigated and reduced [21]. For a country targeted by over 5% of the global cyber-attacks [22], the implementation of an appropriate evaluation model is essential for a UAE Smart Government system which seeks to be fully adopted by 2021 and will cover all scopes of government operations including SCADA systems in utility and sensitive economic sectors [23]. The present study is therefore of critical contribution of the UAE Government's agenda to remain the top of AI and technology exploitation within the region and on the global terrain.

III. Literature Review

March - April 2020
ISSN: 0193-4120 Page No. 931 - 937

A. Theoretical Frameworks of AI and Public Safety Systems

Large scale disagreements surround the underlying concepts and theoretical underpinnings of artificial intelligence evaluation models. Theorists simply assume their own way of evaluation which fits the context of their enquiry. This has inadvertently led to the creation of multiple conceptual foundations based on psychology, neurobiology, engineering, logic and optimisation, and the theory of complexity [24][25]. The complex adaptive systems [26][27], the philosophy and theory of artificial intelligence [28], a grand unified theory of AI [29], and a decision theory of AI [30], are some of the few theoretical per relevant to explaining the relationship between AI and public safety.

The complex adaptive systems theory is considered most critical to the present paper, building on the theory of complexity [26][27]. This theory helps explain both the complexity associated with AI replication of human neural networks and the complexities associated with public safety within integrated societies. Ref [31] asserts that AI was originally introduced to address the complex scenarios and delivery of skills encountered in the management of work activities. AI modulators help address complex systems in the shorted possible time with little to no human intervention.

In the area of public safety management, Ref [32] observes that public safety is a rather complex phenomenon. Public safety exists within the larger social scope and risk to the public must be seen from multiple perspectives of people (social risks), technological development (technical risks) and environmental risks (natural disasters and hazards) [33]. Moreover, [32]:

> "The high number, and variety, of units involved in the systems, intelligent agents, constant solving, and search [43].
>
> All these systems have their strengths and weaknesses in specific contexts. External defence systems include but not limited to service provider security solutions including network firewall protection against external attackers. This includes the system-wide security network adopted in the UAE [20].

D. AI-based Attack-Defense Matrix

With little to no human intervention, an evaluation matrix of an AI-based cyber-attack and defence model is presented in Table 1.0.

TABLE I. A HOLISTIC PERSPECTIVE OF AI-BASED CYBERSECURITY

AI in Cyber Defense		
External (Cyber sabotage)	Cyber sabotage threat versus Cyber-defense systems	Cyber sabotage threat versus cyber architectural defence systems
Internal (Self-Generated Threat)	Cyber-defence versus Cyber self-generated threat	Effective Cyber architectural defence versus internal self-generated threat

execution of actions, the level of interactions occurring between elements, interdependencies produced by linking certain tasks, and adaptation to the environment underlying learning... adds to the complexity of public safety management systems."

It is imperative to note that public safety and AI systems interrelate with other systems and with their surroundings [34].

B. Internal AI malfunction threat and external cybersabotage

AI in Cyber attacks
External (Cyber- defense)

Internal (Architectural Defense)

Ref [35] in a multi-dimensional threat classification of AIindicate that AI threat has both internal and external threat perspectives. Each of these threat classification models has both accidental and planned threat intents. Internal threat intents represent threats that are introduced without external actors. These include AI system self-alterations resulting from data corruption and accidental modifications. Two examples in this area include "Tay" — a Microsoft Twitter bot that went racist within 24 hours after being unleashed onto Twitter [36], and the Deep Learning Interface for Accounting (Delia), an AI accounting bot that automatically created bank account and siphoned customer's monies into these accounts [37].

From an external attack perspective, threat is as a result of AI-based harmful actions launched by parties external to the SCADA systems [35]. Evidence exists on permanent and temporary AI-based cyber troops in over 100 governments globally [38]. The remote infrastructure attacks on Estonia and Ukraine power lines are evidence of state-backed actors' attempts to seize control SCADA, remotely switch off power stations, destroy important files stored on servers, disable and cause destruction of IT infrastructure components by altering gauges, among others [39][40][41]. To uncover flaws, external actors use AI-Agents in a concurrent manner; Estonia and Ukraine saw intelligent malware such as the BlackEnergy and the KillDisk evident throughout the attacks [42].

C. Internal AI architectural defence and external defence systems

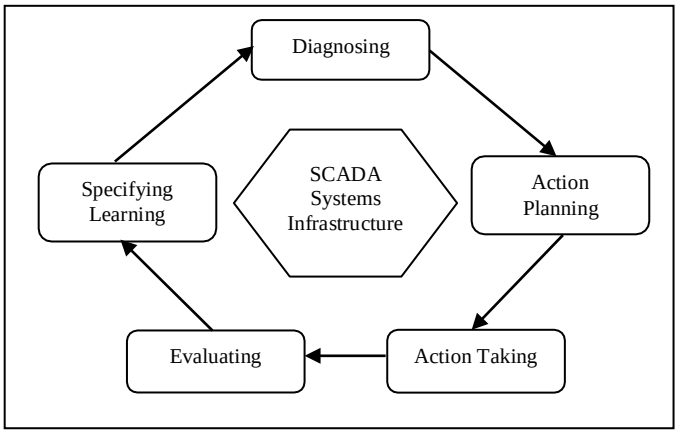
The AI-based cyber-security landscape has key defence blocks within the architectural, passive and active defence scopes [40]. The technology system architecture remains at the core of the AI defence framework – this constitutes the planning, establishing and upkeep of technology systems with security in mind [40]. According to Ref [43], internal or architectural system AI-defense range from neural nets, expert This matrix does not consider human intervention and completely relies on the installed efficiencies of AI. Humans are relevant mediators of the effectiveness of technology systems. With AI in charge, humans are regressed to a monitoring or governance position. AI and automation nearly are increasingly offered control over industrial systems operationalization and emergencies.

March - April 2020
ISSN: 0193-4120 Page No. 931 - 937

IV. Methodology

Action Research was used as the overall research strategy for the present paper (Fig.1) as originally proposed by [44]. This paper covers the first two stages of action research and reserves the three stages for future research. on a consolidation of all relevant literature presented.

Figure 1. Action Research Process



Two (2) main SCADA Control Rooms are considered central to this paper. These SCADA control rooms handle a good amount of physical and infrastructural systems installed across the Emirate of Abu Dhabi. The results commence with a careful diagnosis of existing systems from the client and control room perspective, mainly within the help of document analysis and informal interviews. Action Planning entails careful matrix modelling of possible courses of actions that balances AI defence and attacks in the SCADA environment. In Part Two of the paper, the SCADA Control Rooms are carefully observed and evaluated using this model. Specific learnings are then presented.

V. Results and Discussions

A. Diagnosis – Document Analysis and Interviews

The study commenced with a document analysis of SCADA security protocols and memorandums between the SCADA control room operators and the clients. The documents provide key criteria for systems security monitoring, maintenance, and protocol in emergency situations. Both system and humans' aspects of the SCADA security systems are clearly specified. These cover all areas of system configuration, staff awareness, training and general security measures including authentication bypass vulnerabilities.

A total of three (3) informal interviews were conducted as part of the present study. Two interviews were conducted with selected specialised employees with the SCADA control rooms, whist the last interview was conducted with a client representative. Insights revealed that awareness of security breaches and attack approaches used by external actors is critical to present outsiders from gaining inside access to the systems. Phishing and sending out malicious codes and links to the email addresses of the SCADA control room employees is a typical external attack point. To control internal malfunctions, AI must not be offered excessive control over SCADA systems, and human monitoring is critical.

Understanding policy requirements through frequent security quizzes are critical to keeping the specialised and other staff become abreast with the latest industry threats and developments. It is also important that security performance metrics are maintained in the form of KPIs. The KPIs include both system and human performances. Regarding the system, false positives must be reduced to the barest minimum in optimal performance. According to one respondent:

> *"If an oil pipeline goes under or around an airport, the AI system must be able to differentiate between an earthquake and the landing of an aeroplane. Raising emergency termination of utility service due to a wrong stimulus has dire consequences and cost effects.*

This observation or scenario counts as an accidental threat to the installed systems emanating from an inside source or a system malfunction. In one other elaboration:

> *"Attackers try to gain access through the control portal... this helps them send wrong signals, change valve readings and send misinterpretation of field events to the system and those conducting the monitoring.*

Public safety is paramount to the operations of the SCADA and the client needs. Participants referred to historic events of oil & gas pipeline explosions due to the lack of proper interpretation in monitoring and security protocol considerations. Most importantly, these flaws have had severe consequences on public life. The use of high-tech sensors cannot always be trusted as evidence exist that most leaks go un-noticed despite high-tech AI monitors.

B. Action Planning – Evaluation Matrix

At this stage of the research, the evaluation matrix was prepared using relevant cues gathered from the earlier diagnosis. The matrix consists of dual perspectives of attack and status and an outcome of public safety. Both attack and defence security status take on three main security mechanisms of an internal, external and human governance role. A suitable mechanism is generated to define each status – whether attack or defence. It is imperative that critical defence mechanisms are active to counterattack nodes, to guarantee public safety. Within each mechanism, system and staff roles are specified. Various definition leading to the model are presented.

Definition 1:

P is an AI-based security scope enhancing or degrading public safety. Two main scopes are considered in a mix that affects public safety, where:

P_1: All attack scenarios that define a scope relevant to public safety

P_2: All defence scenarios that defines a scope relevant to public safety

March - April 2020
ISSN: 0193-4120 Page No. 931 - 937

Definition 2:

M is the security mechanism used to define any aspect of the security scope. In principle, there may be more than one mechanism to effectively define an attack or defence scope. Therefore, a P_1 can be addressed by a list of mechanisms M_1, M_2… M_β), where is the maximum number of security mechanisms supported within a scope. The following are presented:

M_1: Mechanisms Internal to the SCADA system within any defined scope

M_2: Mechanisms External to the SCADA system within a defined scope.

M_3: Human governance role within a defined scope; a critical mediator of attack and public safety

$$\langle P_1, M_2 \rangle \rightarrow S^{sys}_{(a,b,c\ldots z)_{\langle P_1,M_2\rangle}}$$

$$\langle P_1, M_3 \rangle \rightarrow S^{sec}_{(a,b,c\ldots z)_{\langle P_1,M_3\rangle}}$$

Definition 3:

S is the system or staff responsible for addressing

$$\langle P_2, M_1 \rangle \rightarrow S^{sys}_{(a,b,c\ldots z)_{\langle P_2,M_1\rangle}}$$

$$\langle P_2, M_2 \rangle \rightarrow S^{sys}_{(a,b,c\ldots z)_{\langle P_2,M_2\rangle}}$$

a security mechanism M within a defined scope P. The responsible party can be categorized into at least two types:

a. **Security Team** – this is labelled as S^{sec}, and represent staff specialised in IT of the SCADA Control room management and Client Portal Security. Considering the following

S^{sec1}: Control room supervisor – full access control S^{sec2}: Control room assistant – partial control

S^{sec3}: Client company infrastructure supervisor

b. **System –** System operating mode, labelled as S^{sys}, including internal and external system behaviour.

S^{sys1}: Internal AI system integration

S^{sys2}: Internal Robot Process Automation (RPA) systems S^{sys3}: External AI system

Multiple security systems and teams may be responsible for different aspects of the mechanism; therefore, $S^{sec} = S^{sec1}$, S^{sec2}, …, ^{secmax}, an indication of all security team members in the Control Room and the Client organization responsible for the security mechanisms. Likewise, more than one system may be in charge of operationalizing any security mechanism; therefore, $S^{sys} = S^{sys1}$, S^{sys2}, , ^{sysmax}, an indication of all security systems responsible for all security mechanisms.

All security team members (S^{sec}) and systems (S^{sys}) have an unlimited number of specific functions. Let each function be represented by a, b, c, d…. z where z represents the last most important function necessary for the security mechanisms and performed by the system or the security team.

Definition 4:

Considering two scopes necessary to define any public safety outcome, the three security mechanisms handled either by the system or the security team. The state of public safety for any SCADA system is, therefore, a combination of specific functions addressing all security mechanisms required by every scope necessary for the achievement of public safety:

$$\sum_{i=1}^{\alpha}\sum_{j=1}^{\beta_j}\langle P_i, M_j \rangle \rightarrow S^{sec\,|sys}_{(a,b,c\ldots z)_{\langle P_i,M_j\rangle}}$$

Building on this model, the total amount of Scope-Mechanisms that can be mapped onto appropriate roles. Three main attack sequences may be established; the first two sequences of internal and external security mechanisms are handled only by the system. Humans can mediate attacks but do not stand a chance as defence agents alone. All attack scope-mechanism combination is therefore presented as follows:

$$\langle P_1, M_1 \rangle \rightarrow S^{sys}_{(a,b,c\ldots z)_{\langle P_1,M_1\rangle}}$$

All defence Scope-Mechanisms scenarios are presented below.

Human intervention only takes the form of attack mediation and does not play an active role in defence, since human defence against AI can only be at least not until an attack has been recorded or suspicion registered. Given these scope-mechanisms scenarios, a brief example of the AI evaluation matrix is presented in the next section to help understand key components oof this observation.

A. An Example

Assuming 3 main attack functions are relevant to $\langle P_1, M_1 \rangle$ and these functions include system resilience to false positives, human controllability, and resilience to malfunctions. The level provided for each of these functions is only 2 (yes/no). The state of each of the three system modes for all three functions will be presented as follows:

$<P_1M_1>$	Attack-Internal Resilience		
System ID	Resilience to False positives (a)	Human controllability (b)	Resilience to malfunctions (c)
S^{sys1}	Y	Y	Y
S^{sys2}	N	Y	Y
S^{sysall}	N	Y	Y

$<P_1M_1>$ is No if any single system function is No. The system works together, and a single vulnerability in an installed component grants access to attackers.

For $<P_1M_2>$, all external attacks are measured. The three most important functions here include authentication bypass, brute force vulnerability and malware vulnerability. The scope-mechanism for these functions are presented::

$<P_1M_2>$	Attack-External Resilience		
System ID	Authentication bypass vul. (a)	Brute Force vul. (b)	Malware vul. (c)
S^{sys1}	Y	Y	Y

March - April 2020
ISSN: 0193-4120 Page No. 931 - 937

S_{sys2}	Y	Y	N
S_{sysall}	Y	Y	N

<P_1M_2> is No if any single system functions is weak to external attacks.

For <P_1M_3>, the role of humans is brought into perspective. For humans, the three most important functions include threat awareness, threat training, and IT self-efficacy. For the third mechanism for the attack scope, the following is established:

<P_1M_3>	Attack- Resilience – the role of humans		
System ID	Awareness (a)	Training (b)	Tech Efficacy (c)
S_{sec1}	Y	Y	Y
S_{sec2}	Y	Y	N
S_{sec3}	Y	N	N
S_{secall}	Y	N	N

The overall attack scenario is presented as follows:

	<P_1M_3>	<P_1M_3>	<P_1M_3>
a	N	Y	Y
b	Y	Y	N
c	Y	N	N

For the defence scope, two other combinations are required. The first of these is defence scope and internal mechanism combination <P_1M_2>. We can generate the defence-internal matrix using the top three functions of neural nets, learning and search.

<P_2M_1>	Defence – internal		
System ID	Neural Nets (a)	Learning (b)	Search (c)
S_{sys1}	N	Y	Y
S_{sys2}	Y	N	Y
S_{sysall}	N	N	Y

The external defence matrix can also be generated

<P_2M_2>	Defence – External		
System ID	Firewall (a)	Encryption (b)	Track/Trace (c)
S_{sys3}	N	Y	Y

using the following:

Overall defense matrix is given as follows:

	<P_2M_1>,	<P_2M_2>,
a	N	N
b	N	Y
c	Y	Y

Given the attack and defence scenarios, the final matrix is given as:

	Attack				Defense			Safety
	Ext	Int	Hum	P_1	Ext	Int	P_2	Public Safety
a	N	Y	Y	40%	N	N	0%	40%
b	Y	Y	N	40%	N	Y	20%	60%
c	Y	N	N	20%	Y	Y	40%	60%

C. Discussion and Conclusion on AI-SCADA, Human Technology Governance, and Public Safety

The mandate of AI in SCADA is clear; this technology is focused on system monitoring, data collection, and control centring. These functions help monitor traditional technology systems and RPA expert systems in the bid to collect data, learn from events, study patterns, and take control measures necessary. In the area off utility SCADA systems, separate pools of evidence support system attack vulnerability analysis [45][46], the development of countermeasures for defence [47][48], and consequent analysis including public safety [49]. The present paper captures all three phases in a singular matrix and can be used for real-world cases public safety evaluation.

The vulnerability of SCADA systems is directly linked to public safety as the public become increasingly dependent on infrastructural systems. The matrix can be applied to existing SCADA systems to measure the degree to which top security functions are vulnerable or threaten overall public safety. After applying the evaluation model, key learning may be established.

REFERENCES

[1] Choenni, S., Leertouwer, E. (2010). Public Safety Mashups to Support Policy Makers. In K.M. Andersen, E. Francesconi & A.G.T.M. van Engers (Eds.), Electronic Government and the Information Systems Perspective (pp. 234-248). Berlin Heidelberg: Springer-Verlag.

[2] Tomasino, A., P. (2011). Public Safety Networks as a Type of Complex Adaptive System. In H. Sayama, A. Minai, D. Braha, & Y. Bar-Yam (Eds.), Unifying Themes in Complex Systems (pp. 1350-1364), Proceedings of the Eighth International Conference on Complex Systems. New England: Knowledge Press.

[3] Williams, C., B., Dias, M., Fedorowicz, J., Jacobson, D., Vilvovsky, S., Sawyer, S., Tyworth, M. (2009). The formation of inter-organizational information sharing networks in public safety: Cartographic insights on rational choice and institutional explanations. Information Polity: The International Journal of Government & Democracy in the Information Age, 14, 1/2, 13-29.

[4] Kożuch, B., Dobrowolski, Z. (2014). Creating Public Trust. Organisational Perspective. Frankfurt: Peter Lang.

[5] Patel, S. C., & Sanyal, P. (2008). Securing SCADA systems. Information Management & Computer Security, 16(4), 398-414.

[6] Nicholson, A., Webber, S., Dyer, S., Patel, T., & Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. Computers & Security, 31(4), 418-436.

[7] Research and Markets (2018). Industry Report 2017: Data for 2014-2015, Revenue Estimates for 2016 & Forecasts to 2023. Retrieved from:
https://www.prnewswire.com/news-releases/global-scada-systems-in-oil--gas-industry-report-2017-data-for-2014-2015-revenue-estimates-for-2016--forecasts-to-2023-300578874.html

[8] Kadar, P., Attila, K., Andras, M., & Ervin, S. (1999). Extension of the standard SCADA functionality with AI tools. In Electric Power Engineering, 1999. PowerTech Budapest 99. International Conference on (p. 27). IEEE.

[9] Lange T. (2007). Intelligent SCADA Systems. Automation & Control Technical, Retrieved from:
https://www.researchgate.net/publication/4312695_Automation_and_co ntrol_of_DIA_transportation_tunnel

[10] Williams, T. (2007). Cyber Security Threats to Pipelines and Refineries. Pipeline & Gas Journal, 234(11); 56-58.

[11] Shin, J., Son, H., & Heo, G. (2015). Development of a cyber security risk model using Bayesian networks. Reliability Engineering & System Safety, 134, 208-217.

[12] Abraham, S., & Nair, S. (2014). Cyber security analytics: a stochastic model for security quantification using absorbing markov chains. Journal of Communications, 9(12), 899-907.

[13] Nicol, D. M., Sanders, W. H., & Trivedi, K. S. (2004). Model-based evaluation: from dependability to security. *IEEE Transactions on dependable and secure computing*, 1(1), 48-65.

[14] LeMay, E., Ford, M. D., Keefe, K., Sanders, W. H., & Muehrcke, C. (2011, September). Model-based security metrics using adversary view security evaluation (advise). In 2011 Eighth International Conference on Quantitative Evaluation of SysTems (pp. 191-200). IEEE.

[15] Lala, C., & Panda, B. (2001). Evaluating damage from cyber-attacks: a model and analysis. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 31(4), 300-310.

[16] UAE Government (2018) UAE Artificial Intelligence Strategy.
Retrieved from: http://www.uaeai.ae/en/

[17] Ryan, P. (2018). The UAE will save billions thanks to artificial intelligence, says AI minister. [Online:] Gulf Business. Retrieved from: https://www.thenational.ae/uae/the-uae-will-save-billions-thanks-to- artificial-intelligence-says-ai-minister-1.746041

[18] UAE Government (2019). UAE Centennial 2071. Retrieved from: https://uaecabinet.ae/en/details/news/mohammed-bin-rashid-launches- five-decade-government-plan-uae-centennial-2071

[19] Juma, Y. (2012a). Milipol Qatar 2012 Boasts Record Participation. Nation Shield. [A Specialized Monthly Journal On Military & Strategic Affairs, 41st Year – November, Issue No. 490

[20] Juma, Y. (2012b). Cyber Warfare Integration and Data Protection. A Specialized Monthly Journal on Military & Strategic Affairs, 40th Year
- July, Issue No. 486

[21] Gagne J. F. (2018). Mew Power Means New Responsibility: A Framework for AI Governance. Retrieved from: http://www.jfgagne.ai/blog/framework-for-ai-governance

[22] Zaatari S. (2017). 5% of global cyber attacks targeted UAE last year. Retrieved from: https://gulfnews.com/uae/crime/5-of-global-cyber-attacks-targeted-uae-last-year-1.2027770

[23] UAE Government, (2010).UAE Vision 2021. [Online:] Retrieved from: https://www.vision2021.ae/en/uae-vision

[24] Russell & Norvig 2003, who make the analogy with aeronautical engineering.

[25] McCorduck, P. (2004), Machines Who Think (2nd ed.), Natick, MA: A. K. Peters, Ltd., ISBN 1-56881-205-1.

[26] Comfort, L., K., Dunn, M., Johnson, D., Skertich, R., Zagorecki, A. (2004). Coordination in complex systems: increasing efficiency in disaster mitigation and response. International Journal of Emergency Management, 2, 62-80.

[27] Benbya, H., McKelvey, B. (2006). Toward a complexity theory of information systems development. Information Technology & People, 19, 1, 12 - 34.

[28] Müller, V. C. (2012). Introduction: philosophy and theory of artificial intelligence.

[29] Hardesty, L. (2010). A grand unified theory of AI. Retrieved from: http://news.mit.edu/2010/ai-unification

[30] Feldman, J. A., & Yakimovsky, Y. (1974). Decision theory and artificial intelligence: I. A semantics-based region analyzer. Artificial Intelligence, 5(4), 349-371.

[31] Osoba, O. A., & Welser, W. (2017). The risks of artificial intelligence to security and the future of work. RAND.

[32] Kożuch, B., Sienkiewicz-Małyjurek, K. (2013). Collaborative networks as a basis for internal economic security in sustainable local governance. The case of Poland. In K. Raczkowski & F. Schneider (Eds.), The economic security of business transactions. Management in business (pp. 313-328). Oxford: Chartridge Books.

[33] Tomasino, A., P. (2011). Public Safety Networks as a Type of Complex Adaptive System. In H. Sayama, A. Minai, D. Braha, & Y. Bar-Yam (Eds.), Unifying Themes in Complex Systems (pp. 1350-1364), Proceedings of the Eighth International Conference on Complex Systems. New England: Knowledge Press.

[34] Chiva, R., Ghauri, P., & Alegre, J. (2014). Organizational Learning, Innovation and Internationalization: A Complex System Model. British Journal of Management, 25, 687–705.

[35] Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32, 489-496.

[36] Vincent (2016). https://www.theverge.com/2016/3/24/11297050/tay-microsoft-chatbot-racist

[37] Hatipoglu (2016). AI Steals Money From Banking Customers. http://trendintech.com/2016/04/10/ai-steals-money-from-banking-customers/

[38] Bradshaw, S., & Howard, P. N. (2018). Challenging truth and trust: A global inventory of organized social media manipulation. The Computational Propaganda Project. Retrieved from: https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf

[39] Mansfield-Devine, S. (2012). Estonia: what doesn't kill you makes you stronger. Network security,7, 12-20

[40] Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case. E-ISAC. Retrieved from: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[41] Styczynski, J, Beach-Westmoreland, N., Stables, S. (2016). When the lights went out. Booz, Allen and Hamilton, McLean, Virginia

[42] Finkle, J., (2016) U.S. firm blames Russian 'Sandworm' hackers for Ukraine outage. Reuters.

[43] Tyugu, E. (2011, June). Artificial intelligence in cyber defense. In Cyber Conflict (ICCC), 2011 3rd International Conference on (pp. 1-11). IEEE.

[44] Susman, G. I., & Evered, R. D. (1978). An Assessment of the Scientific Merits of Action Research. Administrative Science Quarterly, 23(4), 582–603.

[45] Dan, G. & Sandberg, H. (2010). Stealth attacks and protection schemes for state estimators in power systems," in Proc. of IEEE SmartGridComm

[46] Teixeira, A., Amin, S., Sandberg, H., Johansson, K. H., & Sastry, S. S. (2010, December). Cyber security analysis of state estimators in electric power systems. In 49th IEEE conference on decision and control (CDC) (pp. 5991-5998). IEEE.

[47] Kosut, O., Jia, L., Thomas, R. J., & Tong, L. (2010, October). Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In 2010 First IEEE International Conference on Smart Grid Communications (pp. 220-225). IEEE.

[48] Bobba, R. B., Rogers, K. M., Wang, Q., Khurana, H., Nahrstedt, K., & Overbye, T. J. (2010, April). Detecting false data injection attacks on dc state estimation. In Preprints of the First Workshop on Secure Control Systems, CPSWEEK (Vol. 2010).

[49] Esfahani, P. M., Vrakopoulou, M., Margellos, K., Lygeros, J., & Andersson, G. (2010). Cyber attack in a two-area power system: Impact identification using reachability. In Proceedings of the 2010 American control conference (pp. 962-967). IEEE.