Proceedings of the 55th Hawaii International Conference on System Sciences | 2022

The AI Family: The Information Security Managers Best Frenemy?

Kristel de Nobrega
Central Bank of Aruba
k.denobrega@cbaruba.org

Anne-Françoise Rutkowski
Tilburg University
a.rutkowski@tilburguniversity.edu

Abstract

In this exploratory study, we deliberately pull apart the Artificial from the Intelligence, the material from the human. We first assessed the existing technological controls available to Information Security Managers (ISMs) to ensure their in-depth defense strategies. Based on the AI watch taxonomy, we then discuss each of the 15 technologies and their potential impact on the transformation of jobs in the field of security (i.e., AI trainers, AI explainers and AI sustainers). Additionally, in a pilot study we collect the evaluation and the narratives of the employees (n=6) of a small financial institution in a focus group session. We particularly focus on their perception of the role of AI systems in the future of cyber security.

1. Introduction

Hyperautomation deals with the application of Artificial Intelligence (AI) and subdomains such as reasoning, planning, machine learning, natural language processing and robotics. Autonomous things exploit AI to perform tasks usually done by humans, while offering increasingly AI-driven decision-making capacity. The aim of AI systems is to increase human well-being [1]. Nonetheless, in 2013, Paul Krugman [2], Nobel Memorial Prize in Economic Sciences, warned that “today, a much darker picture of the effects of technology on labor is emerging. In this picture, highly educated workers are as likely as less educated workers to find themselves displaced and devalued, and pushing for more education may create as many problems as it solves” (p.118). Recently, the European Commission reported that some estimate the number of 2 billion jobs may be lost to automation, while others claim that 375 million jobs will be created by 2025/30 [3]. Hyperautomation and autonomous things will not only substitute human workers but also create new job opportunities. For example, new AI-driven business and technology jobs [4] will emerge and humans will complement the tasks performed by cognitive technology, ensuring that the work of machines is both effective and responsible. AI trainers (i.e., workers performing tasks useful to train AI systems), AI explainers (i.e., workers interpreting the outputs generated by AI systems), and AI sustainers (i.e., workers monitoring the work of AI systems) may be the future jobs of the generations Z and Alpha [4]. This job transformation may happen in the near future.

The results of a recent survey conducted by the European Commission revealed that Europeans are concerned about the impact of robots and AI on employment: 74% of respondents expect that due to the use of robots and artificial intelligence, more jobs will disappear than new jobs will be created. Alternatively, 72% of respondents believe robots steal people’s jobs and 44% of respondents who are currently working think their current job could at least partly be done by a robot or AI [5, 6, 7]. Brynjolfsson and McAfee [8] showed the pace at which technological innovation disrupts labor markets by making workers redundant. The impact of computerization on labor market outcomes is well-established in literature [9]. It documents the decline of occupations mainly consisting of procedural tasks performed by sophisticated algorithms. What is clear is that nowadays, not only routine tasks can be automated, but also non-routine cognitive tasks, such as complex decision-making.

Exploiting or developing sophisticated AI entails new security challenges. AI is both a blessing and a curse for Information Security Managers (ISMs). On one hand, they learn how to leverage AI to enhance security defense. AI allows uncovering patterns of attacks and automating parts of the cybersecurity processes. For example, AI systems focus on assistance of cyber operators [10]. AI supports development of interpersonal skills in cyber decision making and teaming contexts. AI also support the automation of red teaming services [11], for example, through model based, automated cyber red teaming. This increases understanding of impacts that arise from cyber vulnerabilities and proposes a selection of mitigation strategies. Companies can deploy automated AI onto the network as a form of continuous security testing. On the

URI: https://hdl.handle.net/10125/79352
978-0-9981331-5-7

other hand, managers must anticipate nefarious use of AI and defend against them. As Madnick [12] stated, "The good guys are getting better, but the bad guys are getting badder faster" (p.4). AI affects the security space (i.e., increasing surface vulnerabilities) and opens new points of attack across industries. The MIRAI *botnet* attack is an interesting example of a polymorphic malware. Detecting the threat occured through AI technology. At its peak, the Mirai botnet infected over 600,000 vulnerable IoT devices (e.g. home routers, air-quality monitors, and personal surveillance cameras) [13]. Cyber attacks are designed to create confusion and overload the target. Particularly, ISMs are bombarded with computer-processed data linked to cyber-threats. Analysis of the correlation of external scanning data to the network are made every 39 seconds, with an average of 2,244 times per day [14]. ISMs have to analyze spam emails that slipped through the spam filter. Such technical control had already caught about 80-90% of the 16k emails with malicious indicators. Another example of a tedious task is to make sense of internal network traffic which might amount to 400 to 500 alerts per month for a small and simple organization. ISMs have to keep high states of alert for indefinite periods of time [15, 16]. This kind of IT-related overload (i.e., excessive number of inputs delivered through IT) impacts the associated ability in processing the information efficiently and taking proper decisions [17, 18]. Context is required to decide wisely on the actions to be taken. Such decisions may be overwhelming and produce anxiety that may in turn cause inaction or burnout [19, 20]. There is high personnel turnover in the field of security. Particularly, there are consistently high burnout rates for security analysts [21]. ISMs typically focus on security threats through application of formal, informal and technical controls [16]. ISMs have to fight on many fronts to defend their organization. Compliance to formal controls such as, policies, procedures, risk assessments are particularly time consuming. Also, they must cope with insider threats and, through informal control, watch their team [21, 22, 23]. Crucial is the deployment of technical controls that serve as first line of defense such as spam filters. At last, but not at least, the profession requires team collaboration [24, 25]. However, the team responsibility may rely on a few specialists only when resources are lacking. This situation is particularly salient in the context of a small economy [26].

2. The Intelligence and the Artificial

Newell, Shaw, and Simon [27] designed and implemented processing languages that incorporate basic human information processes supported by computer programs such as the Logic Theorist, used to solve difficult problems. Cognitivists reverse-engineered the mind and developed new computational and associative models. Thought processes (i.e., information processing) were no longer considered as part of an inaccessible black box [28]. In 1959, McCarthy joined Minsky and they started the MIT Artificial Intelligence Project [29]. They agreed that the most critical problem was in understanding how minds do commonsense reasoning. The field of AI was mainly founded by the collaboration of McCarthy, Minsky, Newell, and Simon. They coined the term Artificial Intelligence [30]. Their ideas have largely shaped the path of mainstream AI for decades [31]. The aim of AI was originally to duplicate the cognitive and reasoning abilities of humans, building a super powerful computer or robot boasting anthropomorphic cognitive capabilities [32].

What magical trick makes us intelligent? Ask Minsky (1985). "The trick is that there is no trick. The power of intelligence stems from our vast diversity, not from any single, perfect principle" [33] (p.308). Eventually, very few of our actions and decisions come to depend on any single mechanism. Instead, they emerge from conflicts and negotiations among societies of processes that constantly challenge one another" (p. 304). In this article we define Artificial Intelligence (AI) in the terms of McCarthy (1988): "AI is concerned with methods of achieving goals in situations in which the information available has a certain complex character. The methods that have to be used are related to the problem presented by the situation and are similar whether the problem solver is human, a Martian, or a computer program" [34] (p.308).

The concept of decision is in conflict with the idea of a program. Indeed, the artifact designed and programmed does not make the decision. As soon as a task is programmed, the decision no longer exists but is determined by algorithms [35]. Decision-making entails information processing, information structuring, problem-solving and interpersonal communication. Each of these activities represent a succession of goal-driven cognitive and social processes at the individual but also team level [36]. Congruently, an AI system can mimic the decision making process by chunking a large amount of information, but cannot yet substitute the social process embedded in the necessity in making sense of a decision.

We use the following AI system definition [37] "software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information derived from this data and deciding the best action(s) to take to achieve the given goal” (p6). AI systems are a fast-evolving family of technologies (i.e., machine learning, deep learning and neural networks). These are especially important in high-impact sectors (e.g., environment and health, the public sector, finance, mobility, home affairs and agriculture). Productivity gains have been provided to organizations through enhanced computational capabilities and the associated automation of work [37]. “AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behavior by analyzing how the environment is affected by their previous actions.”[38] (p.9). Currently, AI is known for solving well-bounded problems. The solution and the method are completely contained within the data and feedback provided [39]. AI regularly excels beyond human abilities in term of speed and accuracy in processing information. However, AI systems “struggle” when solving problems when additional context is missing while it would be 'common sense' for a human [40]. Part of the context can be provided to an AI in the form of additional data, a model, or human feedback. However, expanding the bounds of the problem is often expensive and may result in poor performance [41].

The AI family counts many 'intelligent' tools. Each one promising to solve problems better and faster than traditional approaches [42]. Incorporating AI into current security systems requires additional skills. Also, hardware and software needs specific human maintenance, AI trainers and AI sustainers. Understanding the nature of the technology is crucial to conclude if 'intelligent' systems will provide a net gain in security. Additionally, AI also introduces additional complexity into systems’ environments. They reduce the ability to understand the behavior of such systems, making them potentially more unpredictable. This unpredictability could introduce new vulnerabilities that could potentially be exploited by hackers. For example, AI software fused with big data analytics and quantum-enabled sensors prove to be able to locate adversary’s submarines easier [43]. ISMs are often confronted with situations where context is leading to take decision while under attack [44]. The risk of being outmatched by an adversary in cyberspace, operating at machine-speed, provides both AI cyber attackers and defenders with few other options than to afford increasingly high levels of autonomy to execute operations. Otherwise, they risk losing the upper-hand in future cyber-attacks – especially attacks that cross the rubric from the virtual to the physical world [45]. Neural network models are at the core of many cybersecurity applications aiming at identifying network attacks by algorithmic intrusion detection [46].

The AI watch taxonomy classifies basic information security tooling by professionals [39]. AI is divided in a wide range of core AI related scientific subdomains (e.g., knowledge representation and reasoning, machine learning) and transversal topics such as applications (e.g., robots, automated vehicles, etc.) or ethical and philosophical considerations. AI categories core and transversal are split up into four AI domains which branch out to sixteen AI subdomains. AI domains reasoning, planning, learning, communication and perception together form the core domain. The transversal domain comprises of integration and interaction, services, ethics and philosophy. The subdomains provide a tangible link to AI systems as known in the security field. It is noteworthy that the suggested domains and subdomains are related, and not disjoint, subsets of AI.

3. Exploratory study

3.1. Technical defense strategies and AI

Security processes in cyberspace deal with the selection and implementation of protection framework and countermeasures. ISMs typically focus on security threats through application of formal, informal and technical controls [47]. Informal controls are defined as behavioral controls, including protection motivation appeals [48, 49, 50]. Formal controls are rule based systems designed to bring uniformity within the organizations. These follow international standards and best practices (e.g., ISACA 1996, SANS institute, NIST, ISO). Technical controls refer to the automation applied as operationalization of formal controls and form a first line of defense. Anti-virus software, firewalls, anti-spyware software, next gen firewalls, Virtual Private Networks (VPN’s), vulnerability/patch management, Security Information Event Management systems (SIEM), Malware Information Sharing Platform (MISP), Intrusion Detection Systems (IDS) and Distributed Intrusion Detection Systems (DIDS) are a few examples of the technical controls currently part of the basic tooling of most organizations [51, 52]. Defending the system is a difficult task for security operations if only the basic set of alerts and follow-up are available. Automating technical controls further could alleviate the load of security staff. Indeed, there is a skill gap in understanding and deciding on alerts [53]. The most challenging part is relieving the burden of decision-making on the ISM. Technological defenses are deployed at the perimeter and network levels as an integral part of the defense-in-depth strategy. The perimeter control (PC) is the outer defensive layer, and is the first one the attacker attempts to penetrate to gain access to the internal network [54]. Defenses should be deployed where hackers cannot trivially bypass them. It should be configured so that a failure of one perimeter has minimal consequences to the overall network security posture [55]. In this article, the PC and the cluster of other internal technical network control layers and countermeasures are referred to as the Internal Controls (IC).

We deliberately pull apart the Artificial from the Intelligence, the material from the human in our exploratory study. We acknowledge the imbrication or entanglement of both agencies are thoroughly discussed in the MIS field [56, 57]. Recently, the Technology Affordances and Constraints Theory (TACT) [58] answers to Zigurs and Buckland's [59] wishes for a theory to understand the fit between tasks and technology. We define tasks as units of work activity that produce output [60]. Fernandez-Macias et al. [61] propose a classification of tasks according to their role in the work process across two different dimensions; the contents of the task and the tools and methods used for carrying out the task. There are different transmission channels that are affected when a human task is replaced by a purely mechanical or digital algorithm-driven machine. Machines can substitute and/or complement human workers. AI systems can evolve towards performing particular tasks such data collection (e.g., retrieval from databases), arguing and counter-arguing in the context of factual evidence (e.g., decision making support), displaying some learning capabilities (e.g. discovery of new attacks) and therefore mimicking occupations being performed by humans. Interestingly, the role of the human is then training the AI systems by providing examples of intelligence when solving a problem (i.e., AI trainers), interpreting the outputs generated by the AI systems adding intelligence (i.e., AI explainers), or monitoring and watching the work of AI systems (i.e., AI sustainers). Table 1 presents an overview of the core technical control systems. It describes how it supports the security operations tasks, specifies the defense perimeter, and relates each 15 technologies to the AI family. We finally reflect on how it affects employees and potentially will transform or substitute the security jobs in the organization into trainer, explainer or sustainer.

Table 1. Core technical control systems and their AI family and AI job example

Core control	**Description and AI subdomains**	**AI family**	**AI Jobs and examples**
Vulnerability scanner (IC)	Hosts or services that execute internal and/or external scans mapped to active vulnerabilities. Planning scheduling, searching, automated reasoning	Fully automated vulnerability assessment leverage AI techniques to produce expert-like decisions without human assistance, and is by far considered the most desirable method of evaluating a system's security [62].	**Explainer** match business context with patching process **Sustainer** promote algorithms that perform well and demotes others
Firewalls (PC)	System to prevent unauthorized access to or from a network. Control access from untrusted to and from trusted network segments. Knowledge representation, automated reasoning, planning scheduling, machine learning.	Next gen firewalls use user behavior based on patterns. Once installed they add additional alerting modeling traffic and combining more security data in a format that combines and merges function (with IDS/IPS and web filters) to other security tools. Decisions are based on policy exceptions remain at the security operations for actions. Near future of firewalls could take over tasks of blocking traffic that is not allowed or suspicious (neural nets).	**Sustainer** promote algorithms that perform well and demotes those that do not **Explainer** help to translate/communicate to the business current state of functioning.
IDS/IPS (PC)	Intrusion detection system/ Intrusion prevention system Scan network traffic for malware signatures. Automated reasoning, machine learning		
Web filters (PC)	Prevent malicious sites or forbidden by company policy to be accessed Automated reasoning, machine learning		
Email filter (PC)	Email filters are indispensable, it filters email traffic to prevent phishing email attacks	Sandbox and email filter [63] technologies are heavily automated and it is merging with AI ML, optimization	**Sustainer** evaluate cost of poor machine performance

	Automated reasoning	and automated reasoning [64] can elevate this technological control into full autonomy mode.	
Sandbox (PC)	This control verifies files and programs prior to deployment in production environment. Machine learning, optimization, automated reasoning		
Canary tokens/ honeypots (IC/PC)	Software to alert when the system has been probed, attacked or breached. Automated reasoning	Honeypot with a level high AI Intelligence would be able to recognize an adversary in its system and automatically be able to modify the environment around the adversary to effectively deceive them [65].	**Sustainer** algorithm based to detect and auto-deploy deceptive behavior **Explainer** gain transparency in functioning of deception, corresponds to business.
File Integrity Monitor (FIM) (IC)	Software that resides on servers in agent or agentless instance to validate if files are altered. Automated reasoning	Heavily automated, signaling currently rule based. Adding pattern and algorithms to these controls will provide a much richer and autonomous technical control with less false positives.	
Endpoint protection/ response (EDR) (IC/PC)	Protection software installed on the end-user computers to guard against cyber attack Automated reasoning, searching	An approach to protect the computer networks that are remotely bridged to client devices. Matching signature and supervision of require many resources. The monitoring can be substituted with AI by pattern matching of (malware) signature databases and threat intel mapped back to the current traffic monitoring. Taking action on the network and decision making will be the next step to eliminate high rate of false positives.	**Sustainer** algorithm based to detect and auto block user from network to stop attack from spreading. **Explainer** gain transparency in functioning of blocking or protection actions, to align that actions correspond to business.
Network traffic monitor (SOC) (IC/PC)	Monitor of network traffic, rule based. Heavily based on rules and also human cognition for investigation of alerts. All sub domains of reasoning, planning, learning	SOC, SIEM and log collector support the detection of cyber incident response process. These technical controls will need to merge into an AI cyber defense process, where human decision making is set to understand context. Substitute humans with enormous capacity to create patterns. Super intelligent systems will need to learn concept and context of the network in order to help with aggregation of logs.	**Sustainer** algorithm based to detect and auto block user from network to stop attack from spreading **Explainer** gain transparency in functioning of blocking or protection actions, to align actions correspond to business. **Trainer** when escalation and communication is needed with the technical teams during incident response. AI function side by side the security teams of should be most close to human understanding.
SIEM (IC)	SIEM is used to capture logs from the network to help detect attacks on the network. All sub domains of reasoning, planning, learning		
Log collector (IC)	Collection of log for multiple purposes; Forensics, Threat hunting Optimization, automated reasoning		
DLP (IC)	Software for prevention of sensitive or critical information to be sent outside the corporate network Machine learning, automated reasoning, searching	Aim to address insider threat, supported by AI domains ML, optimization and automated reasoning, heavily automated, usually signaling security operations rule based [66]. This control works with EDR.	**Sustainer** algorithm based to detect and auto block traffic or files from leaving the organization. Automation economist, cost of poor performance.
Encryption (IC)	A manner to protect data at rest or in transit with secure algorithm. Control is in place to make sure that access is granted to only those that have the right decryption keys. Optimization/ quantum computing	Impacted primarily by quantum computing breakthrough. This will force new quantum proof encryption. Implementation of encryption however remains a human driven and risk based application and implementation. AI could automate encryption based on regulatory compliance (formal control). Yet other parts of the network may have context constraints (legacy systems or performance hinder) [67].	**Sustainer** algorithm based to detect and deploy encryption onto the network.

VPN (PC)	Secure tunnel to the network segment. Optimization	Encrypted tunnel to dedicated segments of the network. This control focusses on privacy of traffic AI will not improve this control, it will with ML transform to include IPS through the VPN, generating alerts and blocking malicious connections automatically.	**Sustainer** algorithm based to detect and deploy encryption of the VPN tunnel.

To conclude, in the context of technical controls, AI will play a prominent part. Human intelligence will be used to mostly sustain (9) or explain AI (5). The line between AI augmented cyber offense and cyber defense will likely remain an obscure one. However, effective defense against attacks by sophisticated polymorphic malware, such as in the case of the Mirai botnet, will require increasingly innovative and self-learning solutions [43]. AI trainers will be necessary in this context.

3.2. Pilot study: Are technical defense strategies, a blessing or a curse?

In this explorative study, we also collected the evaluations and the narratives of six employees working in a small financial institution (FI). In the last years, concerns for cyber security in the public and private sectors have been raised. The financial sector is highly dependent on IT conform to worldwide standards. Threats increase in the banking sectors as more IT leads to more potential security breaches. Cyber resilience is an important prerequisite for economic growth. Cyber threats may affect financial services for tourists and entrepreneurs of small-scale economies. The FI has a monetary and supervisory mandate, with three main areas of operation, including economic policy, supervision and financial operations. As part of our explorative study, we conducted a set of interviews to pilot our research approach and protocol. Two participants are data analysts (DA), another is a statistician (S). In their occupation, they mostly build data pipelines and optimize data structures. The three others are managers, one of the IT Infrastructure and Architecture (IA), the other of Information Security (IS) and overall the third one is responsible for the Research division (R). The pilot focus group had ample technical understanding of AI and cyber security. All have security within their primary or secondary responsibilities and work closely to address them for the primary processes. The session lasted 1,5 hours and was held online. The organization is facing various types of challenges. It is going through a digital transformation, and it is mostly understaffed. They must manage a high level of uncertainty and have reduced resources compared to larger institution of same nature, experiencing overload [15, 16 19, 20, 21]. In this section, we report narratives that illustrate the opinion of the participants on the future role of AI in the security domain and its potential impact on their profession.

During the focus group session, we learned that the employees embrace the idea of AI systems and foresee its impact in the future as a disruptive but also supportive force. Overall, the participants do not fear for their employment. DA stated that “*change will be disruptive with use of AI. Within 5 years there will be more need for people working with algorithms. This may lead to a knowledge gap*”. He added “*within 10 years there will be more autonomous AI taking over human tasks*”. IA added that “*AI will make us adapt to new ways of working*”. S summarizes this overall perception, adding “*AI helps and harms us in a sense. It requires a new level or edge of reasoning*”. As participants underlined, while nowadays there is a need for AI trainer and explainer, it may change in the near future. “*Human input is important for training, making data sets workable. There will be resources needed for algorithms and classification of models to make them work for you. For the short term they will definitely be supportive to our work, not taking it over*” (IS). IA concluded that “*InfoSec will be raised to a higher level to include and create business rules. It will be more a strategic technology in the security arsenal. This will be the hard part. The toolbox of cyber security will evolve into a specialism to keep the organization safe*”. The participants also related to the resources and cost of AI in such context [68]. IS provided example on the trainability *“Image recognition takes 87 hours to learn a model. Model learning and resourcing takes time.”* The participants nicely related to the ethical dimension. For example, R stated that “*AI will not replace ethics. This will need the human call*”. IS added that “*in 10 years I see some countries putting AI systems in jail*”. Indeed, AI may call onto more formal control such as regulation [69]. S summarized wisely the balance between the nefarious and defensive role of AI. *I think data may also become the next target, as these are fed into models and so if you manipulate the data from which AI learns you can breach the system easily*”. The participants are aware of the development in the field. “*The impact on human taking over AI is there for the longer term. This may be accelerated depending on quantum breakthrough*” (IS). Still, they underline the importance of strategy. R for example reported that “*thinking the strategy, the values and ethics are important for the spur of the moment judgement calls within cyber security. There will always be the need for* *someone ultimately to call the shots. I think the human ability to improvise and make quick shots will be important*". The participants were also asked to discuss each of the 15 technical controls and predict whether these will be automated by AI. The degree of agreement is high. They foresee 12 of the 15 to be completely automated by AI (mode value=6). They discussed further VPN. IS stated that "*AI will not improve this control even with VPN implementing a state-of-the-art machine learning based Intrusion Prevention System in the VPN, generating alerts and blocking malicious connections automatically*." IS added "*Politics will kill this. No VPN for you. Forbidden in various countries*". Also, DLP technology was discussed. DLP benefits from self-learning of e.g. security policy is carried out with AI to promote the update of the security policy. DA emphasized that*" the following vulnerability will rise as the data kept is sensitive. Biometric information leaks this is a big issue. So a broad hybrid combination of humans alongside AI and ethics are important to combat the hackers"*. For large data sets it is currently impossible to scan for the manual intervention. This could be completely executed by AI. Humans will simply review actions to adjust when needed.

4. Limitations, future research, and conclusions

In this exploratory study, we focused only on technical controls. However, it would be worthwhile to assess the impact of AI system on formal and informal controls. The situation may turn out to be way more complex on the legal front when considering informal controls. AI systems for example can help predict the occurrences or reoccurrences of actual or potential criminal offences based on profiling of natural persons, assessing personality traits and characteristics or based on collection of past criminal behavior [1]. Such AI systems are considered high risk [1]. EU categorizes high risk AI systems as "those intended to be used as safety component of products that are subject to third party ex-ante conformity assessment, under which security systems can be classified" [1]. Regarding formal control, AI may require more certification that will take away ISMs from their core job. For example, CISSP, CEH, CSFA, certifications imply that ISMs attain, for certain areas of expertise, after years of experience, completing an exam successfully, while adhering to codes of ethics [70]. We collected information in a small and cohesive financial organization as part of a pilot study. The overall positive approach to AI may vary as function of size and workload of the ISMs, the nature of the profession (e.g., data analyst, IS officers) or sectors. It will be worthwhile to interview different stakeholders in the field of security such as security service providers, incident responders and even ISM of critical infrastructure. Also, we aim at increasing the size sample, interviewing key players in the field from similar institutions. A survey is under development. Finally, the social component of decision making was not addressed. However, security is teamwork [24]. In table 2, we provide some examples of micro processes within the domain of cybersecurity as illustration of tasks based on McGrath [71]. Future research addressing the entanglement or imbrication of the material and the human would help to better understand the phenomena of work substitution [72]. We intend to address closely AI affordance and constraints for ISM applying the TACT [58] in full detail. Indeed, as advanced by TACT, one must consider the dynamic interactions between people and organizations and the technologies they use to understand its consequences.

Table 2. McGrath [72] example of information security task

Quadrant	Segment	Micro process example	Material agency	Human agency
I Generate	1.Planning: generate plans	Plan execution of network segment security.	Planning/scheduling, learning	Low
	2.Creativity: creating ideas	Design or create security in depth by plotting creative ideas on how to best secure systems.	Searching, Automated reasoning	High
II Choose	3. Intellective: *One specific correct answer*	Determining if alert is false positive or not.	Automated reasoning	Low
	4. Decision-making: preferred answer is correct answer	Coordinate with team to remove malware found on system.	Commonsense reasoning, ML	High
III Negotiate	5. Cognitive-conflict task: resolving conflicts of *viewpoint*	Establish consensus with fellow IT members on how the facts should be categorized after incident has been resolved.	Commonsense reasoning, ML	High
	6. Mixed motive task: resolving conflict of *interest*	Bargaining with risk owner to implement controls for security or purchase controls/tools.	Knowledge representation, commonsense reasoning, ML	High

IV Execute	7. Contests / battles: resolving conflicts of *power*	Trying to stop/obfuscate an attack as it occurs on the network (Ransomware/lateral movement).	Automated reasoning, ML	Medium
	8.Performance: physical activities and execution of tasks	Writing an incident report. Writing a policy.	Automated reasoning, searching	Low

While facing information overload one may hope Quantum computing and Quantum Information Processing (QIP) will solve the big data issue, helping in managing processes. However, it is clear that the challenge will remain human and collaborative in nature. These QIP technologies are expected to improve computing communication and cryptographic systems [73]. QIP will surely help chunking data and may lead to automatization of some decisions. This futuristic view of "cyber" will be an emerging area of research, with implication in searching in large databases, cloud storage or intelligence repositories. The advantages of QIP will be key to the cyber security. Cyber will not be limited to the ability of a new generation of super-computing in solving the big data problem. At the strategic level, QIP will give superiority. However, as is well-known in the cyber security domain, such technical superiority never lasts due to what is known as the challenge and response mechanism. Data is not information. Information is contextual and to that respect human decision making will remain key to making informed and strategic decisions [74].

To conclude, automation and AI are accelerating the demand for technological skills over the next 10-15 years. Through 2030, the fastest growing need will be for advanced IT and programming skills -- 90% growth compared to 2016, followed by basic digital skills, with an increase by 69% in the USA and by 65% in Europe. Due to the lack of skilled people in the field, the worldwide skills gap in cybersecurity jobs accounted to 2.9 million [3]. In 2020, the job the most in demands are IT security specialists, Information security analysts, Network security engineers, Security engineers, Application security engineers [53]. This heavy employment shortage may explain part of the engagement for AI system in the security domain. More transparency is however required regarding the data chunking and "intelligent" decision. Recently, "explainable AI" garner greater trust and influence in the profession [75]. One participant stated that "*It is inevitable that in the future it will be AI against AI attacking and defending the organization from cyber incidents. The automated attacks will push to have even lower reaction times, triggers and alerts. These all to have adequate front-line defenses*". This statement maybe visionary. Indeed, ISMs may be caught in a vicious cycle: requiring more sophisticated AI to defend against AI led attacks. Professional shift for the profession should be carefully investigated. S. Hawking displayed similar concerns about Artificial Intelligence's (AI). He told the Cellan-Jones for *The BBC* that the full development of AI could spell the end of the human race. He fears "the consequences of creating something that can match or surpass humans. It would take off on its own, and re-design itself at an ever-increasing rate"[76].

5. References

[1] European Commission, "Proposal for a regulation of the European Parliament and the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts." EUR-Lex - 52021PC0206, 2021.

[2] P. Krugman "Opinion | Sympathy for the Luddites" - The New York Times, 2013, pp.118

[3]European Commission "Developments and forecasts of changing nature of work", Published on Knowledge4policy https://knowledge4policy.ec.europa.eu/foresight/topic/changing-nature-work/developments-forecasts-changing-nature-work_en (accessed on 6 June 2021)

[4] H.J. Wilson, P.R. Daugherty, and N. Morini-Bianzino, "The Jobs That Artificial Intelligence Will Create" Mit.edu, 2017 https://sloanreview.mit.edu/article/will-ai-create-as-many-jobs-as-it-eliminates/ (accessed on 11 June 2021)

[5] N.J. Roese, and E. Amir, "Human—Android Interaction in the Near and Distant Future." Perspectives on Psychological Science, 4(4), 2009, pp.429-434.

[6] F.Y. Wang, "Artificial intelligence and intelligent transportation: Driving into the 3rd axial age with ITS." IEEE Intelligent Transportation Systems Magazine, 9(4), 2017, pp.6-9.

[7] EU report "Attitudes towards impact digitisation and automation daily life", Special Eurobarometer 460-Wave EB87.1,2017,https://ec.europa.eu/jrc/communities/sites/jrccties/files/ebs_460_en.pdf, (accessed on 11 June 2021)

[8] Brynjolfsson E., and A. McAfee. The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. New York: W.W. Norton & Company, 2014.

[9] C.B. Frey, and M.A. Osborne, "The future of employment: How susceptible are jobs to computerisation?" Technological forecasting and social change, 114, 2017, pp.254-280.

[10] P. Khooshabeh, and L. Gale, "Virtual human role players for studying social factors in organizational decision making." Frontiers in psychology 9, 2018, 194.

[11] S. Randhawa, B. Turnbull, J. Yuen, and J. Dean, "Mission-centric automated cyber red teaming."

In Proceedings of the 13th International Conference on Availability, Reliability and Security, 2018, pp. 1-11.

[12] S. Madnick, "Preparing for the cyberattack that will knock out US power grids." Harvard Business Review 10, 2017. Pre https://hbr.org/2017/05/preparing-for-the-cyberattack-that-will-knock-out-u-s-power-grids paring for the Cyberattack That Will Knock Out U.S. Power Grids (hbr.org) (accessed on 5 June, 2021).

[13] H. Griffioen and C. Doerr. "Examining Mirai's Battle over the Internet of Things." Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020, pp.743-756.

[14] Study report by the University of Maryland retrieved from, "https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds" (accessed on 6 June, 2021).

[15] A. Ahmad, J. Webb, K.C. Desouza, and J. Boorman, "Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack." Computers & Security,2019, pp.402-418.

[16] A. Ahmad, R. Bosua, and R. Scheepers. "Protecting organizational competitive advantage: A knowledge leakage perspective." Computers & Security 42, 2014, pp. 27-39.

[17] A.F. Rutkowski, and C. Saunders, "Understanding overload: An emotional cognitive model." Proceedings of the 71st Academy of Management Conference: West meets East: Enlightening, Balancing, Transcending, San Antonio: Academy of Management 2011. 6.

[18] A.F. Rutkowski, and C. Saunders, "Growing pains with information overload.", IEEE Computer, 43(6),2010, pp.94-96.

[19] N.J Roese, "Counterfactual thinking.", Psychological Bulletin, 121, 1997, pp.133–14.

[20] J. Wang, Y. Li, and H.R. Rao, "Coping responses in phishing detection: an investigation of antecedents and consequences." Information Systems Research, 28(2), 2017, pp.378-396.

[21] S.C. Sundaramurthy, A.G. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh, and S.R. Rajagopalan, "A human capital model for mitigating security analyst burnout." 11th Symposium On Usable Privacy and Security, 2015, pp. 347-359.

[22] S.R. Boss, L.J Kirsch, I. Angermeier, R.A Shingler,. and R.W. Boss,"If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security." European Journal of Information Systems, 18(2), 2009, pp.151-164.

[23] M. Nicho, and F. Kamoun," Multiple case study approach to identify aggravating variables of insider threats in information systems." Communications of the Association for Information Systems, 35(1), 2014, pp.18.

[24] C.W. Yoo, J. Goo, and H.R. Rao, "Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness." MISQ, 44(2) 2020.pp.907-931.

[25] C.Z. Liu, Zafar, H. and Au, Y.A., "Rethinking fs-isac: An it security information sharing network model for the financial services sector." Communications of the Association for Information Systems, 34(1), 2014, pp.2.

[26] L. Areng, "Lilliputian states in digital affairs and cyber security." The Tallinn Papers, 2014, pp.1-15.

[27] A. Newell, A., J.C. Shaw, and H.A. Simon, "Empirical explorations of the logic theory machine: a case study in heuristic." In Papers presented at the February 26-28, 1957, western joint computer conference: Techniques for reliability 1957, pp. 218-230.

[28] Rutkowski A.F., and C.S. Saunders, Emotional and cognitive overload: the dark side of information technology. Routledge, 2018.

[29] J. McCarthy, M. L. Minsky and N. Rochester, "Artificial intelligence. Research Laboratory of Electronics (RLE)", Massachusetts Institute of Technology (MIT), 1959, pp. 112-152.

[30] J. McCarthy, M.L. Minsky, N. Rochester, and C.E. Shannon, "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence." C.E. 1955, pp.12-14.

[31] P. Wang, "On defining artificial intelligence." Journal of Artificial General Intelligence, 10(2), 2019, pp.1-37.

[32] C. Saunders, and A.F. Rutkowski, "Go for it: Where IS researchers aren't researching." International Journal of Information Systems and Project Management, Vol. 7, No. 3, 2019, pp.5-15

[33] Minsky, M., Society of mind, Simon and Schuster, 1988.

[34] J. McCarthy," Mathematical logic in artificial intelligence." Daedalus, 1988, pp.297-311.

[35] J.C. Pomerol, "Artificial intelligence and human decision making." European Journal of Operational Research, 99(1), 1997, pp.3-25.

[36] M.J. Verhulst, and A.F., Rutkowski, "Decision-making in the police work force: affordances explained in practice." Group Decision and Negotiation, 27(5), 2018, pp.827-852.

[37] AI, HLEG. "High-level expert group on artificial intelligence." Ethics guidelines for trustworthy AI , 2019, pp. 6

[38] P.A. Hancock "Automation: how much is too much?." Ergonomics, 57(3), 2014, pp.449-454.

[39] S. Samoili, M. Lopez Cobo, E. Gomez Gutierrez, G. De Prato, F. Martinez-Plumed, and B. Delipetrev, "AI WATCH. Defining Artificial Intelligence," EUR 30117 EN, Publications Office of the European Union, Luxembourg, 2020, (last accessed 12 June 2021)

[40] Ein-Dor, P., Artificial intelligence: A short history and the next forty years. Emerging information technologies. Thousand Oaks: Sage, 1999.

[41] A. Babuta, M. Oswald, A. Janjeva, "Artificial Intelligence and UK National Security: Policy Considerations" London: Royal United Services Institute, 2020.

[42] Report "Intelligent security tools". www.ncsc.gov.uk., 2019 (accessed on 12 June 2021).

[43] J. Johnson," Artificial intelligence & future warfare: implications for international security." Defense & Security Analysis, 35(2), 2019, pp.147-169.

[44] A. Naseer, H. Naseer, A. Ahmad, S.B. Maynard, and A.M. Siddiqui, "Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis."

International Journal of Information Management, 59, 2021 pp.102334.

[45] S. Chandel, S. Yu, T. Yitian, Z. Zhili, and H. Yusheng, “Endpoint protection: Measuring the effectiveness of remediation technologies and methodologies for insider threat.”International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) 2019, pp. 81-89.

[46] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, “Machine learning and deep learning methods for cybersecurity.” IEEE access, 6, 2018. pp.35365-35381.

[47] Dhillon, G., Principles of information systems security: Texts and cases. John Wiley & Sons Incorporated, 2007.

[48] J. D'Arcy, A. Hovav, and D. Galletta, “User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach.” Information systems research, 20(1), 2009, pp.79-98.

[49] T. Dinev, and Q. Hu, “The centrality of awareness in the formation of user behavioral intention toward protective information technologies.” Journal of the Association for Information Systems, 8(7), 2007, pp.23.

[50] R. Willison, M. Warkentin, and A.C. Johnston, Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. Information Systems Journal, 28(2), 2018, pp.266-293.

[51] R. Richardson, “CSI 15th Annual Computer Crime and Security Survey,” Computer Security Institute (CSI), New York, NY. 2011.

[52] P. Kessel, P.V., “Outpacing change: Ernst and Young’s 12th annual global information security survey.” Ernst and Young, 2009.

[53] S. Hospelhorn,”Solving The Cybersecurity Skills Shortage in Your Organization”, Varonis, 2020, https://www.varonis.com./blog/cybersecurity-skills-shortage/(accessed on 6 June 2021).

[54] D. Kuipers and M. Fabro,”Control systems cyber security: Defense in depth strategies.” No. INL/EXT-06-11478. Idaho National Laboratory (INL), 2006.

[55] L. Cleghorn, “Network defense methodology: A comparison of defense in depth and defense in breadth.” Journal of Information Security, 2013, pp.144-149.

[56] W.J. Orlikowski, S.V. Scott “Sociomateriality: Challenging the Separation of Technology, Work and Organization.” Acad Manag Ann 2008b, pp. 433–474.

[57] P.M. Leonardi “When flexible routines meet flexible technologies: Affordance, constraint, and the imbrication of human and material agencies.” MISQ 2011, pp.147–167.

[58] A. Majchrzak, ML. Markus “Technology Affordances and Constraints in Management Information Systems (Mis)”.Encyclopedia of Man. Theory. 2012, pp. 5

[59] I .Zigurs, BK. Buckland “A Theory of Task / Technology Fit and Group Support Systems.” MISQ 1998, pp. 313–334.

[60] D.H. Autor, and M.J. Handel, “Putting tasks to the test: Human capital, job tasks, and wages.” Journal of labor Economics, 2013, pp.S59-S96.

[61] E. Fernandez-Macıas and M. Bisello, “Measuring The Content and Methods of Work: a Comprehensive Task Framework.” Technical report, European Foundation for the Improvement of Living and Working Conditions, 2017.

[62] S. Khan, and S. Parkinson. "Review into state of the art of vulnerability assessment using artificial intelligence." Guide to Vulnerability Analysis for Computer Networks and Systems. Springer, Cham, 2018, pp.3-32.

[63] S. Douzi, F. AlShahwan, M. Lemoudden, and B. Ouahidi, “Hybrid email spam detection model using artificial intelligence." Int. J. Mach. Learn. Comput 10.2 2020, pp.316-322.

[64] Savin-Baden, M., “Postdigital humans: Transitions, transformations and transcendence.” Springer Nature, 2021.

[65] J.M. Pittman, K. Hoffpauir, N. Markle, and C. Meadows, “A Taxonomy for Dynamic Honeypot Measures of Effectiveness.” arXiv preprint arXiv:2005.12969. 2020.

[66] M. Rouse. “Data loss prevention (DLP),” Available: https://whatis.techtarget.com/definition/data-loss-prevention-DLP (Accessed last: May 16, 2021)

[67] C. Chevalier, E. Ebrahimi, and Q.H. Vu, “On the Security Notions for Encryption in a Quantum World.” IACR Cryptol. ePrint Arch., 2020, pp.237.

[68] I.W. Tsang, J.T. Kwok, P.M. Cheung, and N. Cristianini, “Core vector machines: Fast SVM training on very large data sets.” Journal of Machine Learning Research, 6(4), 2005, pp.363-392.

[69] N.A, Smuha, “From a ‘race to AI’to a ‘race to AI regulation’: regulatory competition for artificial intelligence.” Law, Innovation and Technology, 13(1), 2021, pp.57-84.

[70] N. Lim, N” Escaping the computer-forensics certification maze: A survey of professional certifications.” Communications of the Association for Information Systems, 23(1), 2008, pp.547-574.

[71] McGrath J.E., Groups: Interaction and performance (Vol. 14). Englewood Cliffs, NJ: Prentice-Hall, 1984.

[72] H. Medina, M. Verhulst and A.-F. Rutkowski, "Is It HIT? Task Complexity and Work Substitution", Proc. 2015 Americas Conf. Information Systems, 2015, pp.1-13.

[73] Gardner, H., The mind's new science: A history of the cognitive revolution. Basic books, 1987.

[74] Damasio, A.R. Descartes’ Error — Emotion, Reason and the Human Brain, New York: Putnam 1994.

[75] D. Gunning, D., “Explainable artificial intelligence “Defense Advanced Research Projects Agency (DARPA), 2017.

[76] R. Cellan- Jones “Stephen Hawking warns artificial intelligence could end mankind”,https://www.bbc.com/news/technology-30290540 ephen Hawking warns artificial intelligence could end mankind - BBC News, (accessed on 5 June 2021).