PRIVACY IMPLICATIONS OF AN AUTOMATED CYBER SECURITY SYSTEM – WITH OR WITHOUT THE HUMAN IN THE LOOP

Introduction

'Star Wars' is the classic example of a symbiotic human-machine relationship. The 'force' guided the human actions which were supported by data driven inputs from the 'droids'. Being guided by the 'force' is nothing, but human ability to use our intuition and exercise judgement. Though a work of fiction, the classic, might have essential food for thought for the future of human-machine interaction!

21st century is the age of automation. Growing emphasis on efficiency, cost effectiveness and freeing the humans of the mundane jobs for more creative activities are driving this trend. Technological advancements like full fibre connectivity, 5G, Internet of Things (IoT) and Big Data revolution are catalysts for this change. While automation has potential to enhance productivity across various sectors, one industry that has appeared as an early deployer of automation is Cybersecurity.[i] Cybersecurity is defined as securing electronic information and information technology devices. This could include data, computers, mobile devices, servers, networks.[ii]

The early deployment of automation in cybersecurity is driven by the large scale of automated cyber-attacks, existing cybersecurity skills gap and complicated and arduous security processes. Functions like data sequencing, data correlation, creating and implementing faster threat protections, detecting existing infections in one's network can be better dealt by automation that humans.[iii] However, demand for cybersecurity automation should not be sufficient to implement it. It is critical to understand the challenges in automating cybersecurity systems and to draw insights from it to inform policy and regulation. This essay aims to do so. The question being asked is: ***What are the privacy implications of an automated cybersecurity system – with or without the human in the loop?***

Privacy is an essential human experience. Right to privacy is stipulated as a fundamental right under Article 12 of the United Nations Declaration of Human Rights (UDHR). Privacy helps us to manage our boundaries and avoid unwarranted interference in our lives. Privacy breach is defined as the access to our bodies, places, and things without our permission.[iv] However, with the Big Data revolution privacy breach has essentially taken the form of data breach as various aspects of our lives are now stored as data with the increasing use of digital technologies. Thus, for the purpose of this essay privacy breach implies data breach.

Human in the Loop (HITL) is a branch of Artificial Intelligence (AI) that leverages both human and machine intelligence to create machine learning models. It comes into play when the machine alone cannot provide the correct answer to a problem and needs human intervention.[v],[vi]

The following section addresses the implications of privacy breach in automated cybersecurity systems with or without the involvement of a human. Key issues are discussed from a philosophical, ethical, social; political; economic; technological and environmental perspective. This is followed by the analysis section that investigates this discussion and provides key insights. The conclusion and recommendation section suggests a way forward.

Key Issues and Debates

The approach adopted in this section is binary i.e. it contrasts the views of the advocates of Technological Determinism and Social Constructivism which are the two leading theoretical camps in the field of Science and

Technology. Technological Determinism assumes that technology determines the development of a society's social structure and cultural values.[vii] Social Constructivists on the other hand contradict this view and emphasise that human action shapes technology and not the other way round. They stress on the fact that the way a technology is used cannot be comprehended without understanding its social context.[viii]

The presentation of the views below is deliberately caricatural to facilitate the understanding of the analysis.

Philosophical, Ethical and Social

Privacy vs security

Privacy is an essential human experience. It helps us to manage our boundaries and avoid unwarranted interference in our lives. Despite the significance of privacy in our lives, there might be occasions when other issues could take priority. Cybersecurity could be one such situation[ix] where there might be a need for the individuals, businesses, or governments to allow monitoring of their networks or devices to prevent a future theft. In this process, it is possible that individuals' personal data might be monitored as well.

In such a situation, Technology Determinists would argue that automation might be critical. This is because having no human interaction would ensure that people's individual data is safe because machines would not see the innate value of the data as humans would. On the contrary, Social Constructivists would argue that humans are the ones who understand the true value of privacy and not machines. Thus, they would be best suited to protect it for others. After all, the hacker is a human too and thus a human mind is truly capable to understand his/her strategy and avert any attacks from happening in the future.

Human well-being, peace, and happiness

Cyber-attacks can cause social disruption to people's lives. They could exacerbate anxiety, feelings of fear and loss of public confidence in technology.[x] Therefore, Technology Determinists would argue for automating cybersecurity systems as according to them that would reduce the risk of privacy breach and resulting social disruption. Without the threat of any theft, people have a greater chance of living their lives in peace and happiness.[xi]

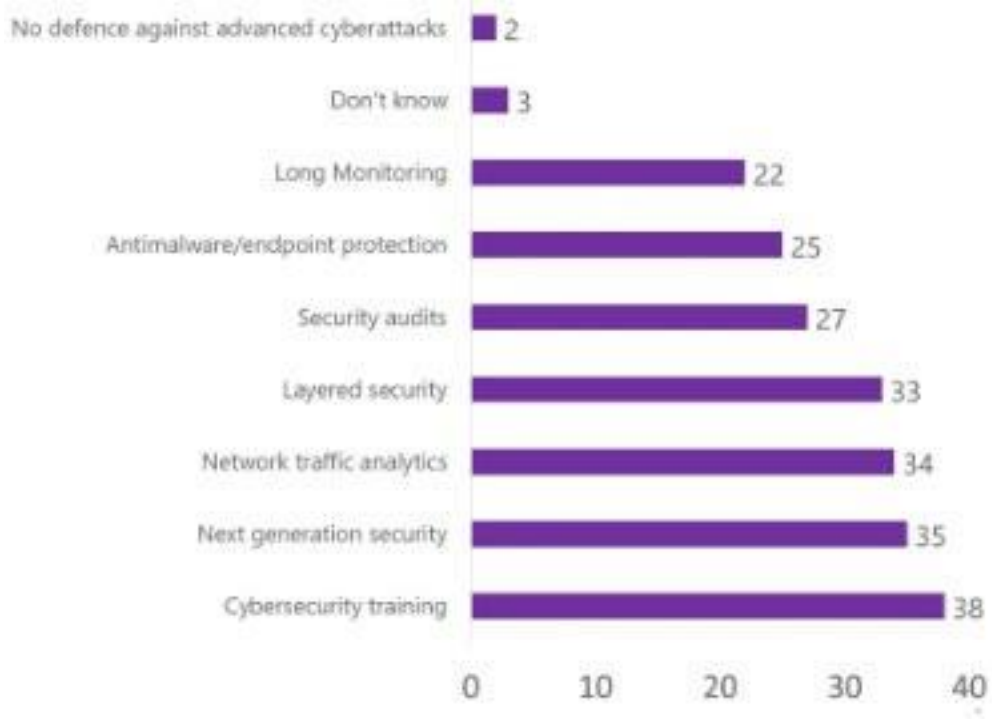
While the Social Constructivists would see the social value that automated cybersecurity systems can bring, they would insist that this is possible only if there is human involvement as lack of transparency in the functioning of the fully automated cybersecurity systems might not get public acceptance. This is because people tend to trust people over machines.

Human as the weakest link

Technology Determinists would argue that humans are the weakest link when it comes to privacy breach. According to a study by IBM, human error is the reason behind 95% of the cyberattacks. These could be an honest mistake of misdelivering a message to a wrong recipient, negligence, lack of knowledge, or even wrong intentions.[xii] Therefore, if there is no human hand, the chances of privacy breach would be minimal.

Social Constructivists would consider this an impractical approach based on a misrepresented reality. They would claim that it is incorrect to identify humans as the weakest link. This is because humans still control most of the security systems, monitor valuable data and use vulnerable machines and software. Therefore, if humans are the only ones who perform these roles, they would be the only ones who make the mistakes as well.[xiii],[xiv] Hence, the solution does not lie in fully automating the systems but rather in educating and training people to make them aware of the best practices in the cybersecurity space. According to a 2019 report by Bitdefender, IT professionals put the highest emphasis on cybersecurity training of their employees to defend against cyber-attacks.[xv] See Figure 1 below.

Figure 1: Preferred security defence mechanism (percentage) [xvi]



Human judgement vs data analysis of a machine

Data is an extremely valuable commodity in the 21st century. Increasing use of digital technologies allows various aspects of our lives to be stored as data. This could include our personal, business, and financial exchanges. According to some reports, people are generating 2.5 quintillion bytes of data every day and nearly 90% of all the data that we have today has been generated in the last two years.[xvii] Therefore, to manage this sudden data explosion, we need significant computing power. Human minds are not designed to analyse this mammoth amount of information. Technology Determinists would argue that fully automated AI systems like Machine Learning (ML) and Deep Learning (DL) would play a critical role in analysing this significant amount of data and provide valuable insights.[xviii],[xix] Also, unlike humans, these machines do not see the innate value of this data and therefore there is no scope of any privacy breach.

The Social Constructivists would argue that even if there is no human interaction, there is no guarantee that a privacy breach will not occur. This is because whether there are no humans inside the loop, there are humans all around the loop. Stakes to make profit will always be human. Therefore, we need humans as they understand human behaviour the best and can pre-empt what the hacker might be thinking using their judgement. According to various reports, fully automated AI systems have output accuracy of only 80%, which can be significantly improved with the involvement of human inputs.[xx]

In a lot of instances, humans play the role of a whistle-blower and prevent many thefts from happening. US Department of Justice and US Securities and Exchange Commissions (SEC) have developed a whistle blower rewards program.[xxi] There have been various cases where poor cybersecurity practices that could significantly increase the chances of privacy breach have been brought to the fore by people. These include July 2019 allegations on Cisco systems for selling vulnerable video surveillance software to government agencies, that put these agencies at risk of unauthorised access. April 2019 allegations on Fortinet to supply the government with poor quality products with doctored product labels.[xxii] This trust in human judgment is echoed by the 2020 report by the Ponemon Institute and Domain Tools. According to the report 68% of the respondents who were IT and security practitioners believe that human involvement is necessary in IT security.[xxiii],[xxiv]

Political

Need for Transparency:

Technology Determinists would argue that complete automation works in an objective and transparent manner, wherein the data inputs that are fed into the algorithms are processed to create products and services without any scope of data manipulation or meddling on the way.

Social Constructivists on the other hand talk about the lack of transparency resulting from completely automated cybersecurity systems. According to them, complete automation would increase the risk of privacy breach due to lack of visibility of the AI algorithm. Whether the privacy breach occurs due to some error in the algorithm or someone from outside hacks into the system, the fact that there would not be someone to monitor this, would increase the risk of breach. Privacy breach underpinned by lack of transparency will have detrimental political consequences. Some reports have pointed out that lack of transparency in AI functioning can erode its public acceptance. If there is no public acceptance for something, it is usually very difficult to gather political acceptance for the same. And political support is important for an industry to grow.[xxv]

Need for Accountability

Accountability is essentially a state of being responsible for one's actions. At the national level, governments put in place processes for accountability of their own executive and others, including citizens to ensure fairness and justice for the country. Technology Determinists would argue that the question of accountability might not even be relevant as no human interaction would mean no scope for privacy breach and hence nothing to be held accountable for. However, that might be far from the reality. There are various reports to show that despite no human errors or wrong intentions, automated cybersecurity systems are getting hacked. It has become a war between one algorithm hacking into the other algorithm.[xxvi] In this situation the Technology Determinists might cede into having some human involvement to ensure monitoring and accountability when needed.

The Social Constructivists, however, would emphasise on function allocation of the HITL model in cybersecurity systems. Function allocation implies clearly distinguishing between the actions performed by a human and a machine within an automated system.[xxvii],[xxviii] They argue that humans in the loop should not only be a mere rubber stamp, rather they should have agency to influence the functioning of the algorithms. There have been known cases where various firms only include humans in the otherwise fully automated cybersecurity loop to avoid regulatory accountability. For example, in case of right to explanation for the output of the algorithm in GDPR. Right to explanation is an individual right under GDPR, according to which an individual can seek the explanation on the outcome of an algorithm. Social Constructivists would argue that if humans do not have complete agency within these automated cybersecurity systems, they wouldn't fully understand how it works and making them accountable or liable for an error, as privacy breach would not be fair. [xxix] Lack of accountability would be another reason for the possible lack of public and political acceptance.

Economic

Rising need and high cost of cybersecurity systems

According to a 2017 Gartner survey cybersecurity needs are on a rise. This is underpinned by factors like – rising privacy concerns, security risks, regulatory changes, and cybersecurity skills shortages.[xxx] Cybersecurity systems are complex and demand high investment. They need one to have the knowledge and familiarisation with numerous security tools. According to a 2016 report by CSOOnline, on average an enterprise uses 75 security tools. This boils down to a significant cost for the companies. [xxxi],[xxxii] According to 'State of Cybersecurity survey (2019), by

ISACA, 87% of the respondents admit that they need an additional 50% of the budget for their cybersecurity systems.[xxxiii] According to some recent studies, average cost of a data breach to small business can range from $120,000 to $1.24 million and for medium to large businesses it can be as high as $3.92 million.[xxxiv]

Cybersecurity skills gap

There is a paucity of cybersecurity professionals.[xxxv] In a 2018 survey by the Enterprise Strategy Group (ESG), 51% of the respondents reported that their organisation had a shortage of cybersecurity professionals.[xxxvi] Primary reason for this scarcity of cybersecurity talent is the mismatch between the demand and supply in the sector. While the attacks have risen in sophistication and scale, cyber specialists coming out from schools and training programmes have not kept up with this trend. The lack of resources at the educational institutions underpins this mismatch as many schools lack trained teachers or course materials in cybersecurity. Lack of a defined career path and the negative reputation of the sector could be other factors deterring young professionals from seeking formal employment in the cybersecurity sector.[xxxvii]

Scale of threat

Scale of the cybersecurity attacks have risen manifold in recent years. As per a 2019 study by Accenture, security breaches have increased by 67% between (2014-2019).[xxxviii] According to a 2014 study by Symantec, 14 adults are targeted by a cyber-attack every second i.e. more than one million attacks every day.[xxxix] These numbers are expected to have increased exponentially by now especially with the advent of automated cyber-attacks.

Based on the above discussion, Technology Determinists would argue that it is critical to automate cybersecurity processes in the light of high scale of automated cyberattacks, rising privacy risks, high cost to the companies, and cybersecurity skills gap. As per a report by Accenture/Ponemon, security automation can combat the risk of rising cost of attack discovery with savings of $2.09 million.[xl] However, while recognising the need for some degree of automation in the cybersecurity systems to deal with the scale of threat, Social Constructivists would emphasise upon the need for training employees. As previously mentioned, according to a 2019 report by Bitdefender, IT professionals put highest emphasis on cybersecurity training of their employees to defend against cybersecurity attacks.[xli] Figure 1 above illustrates this.

Technological

Thinking machines

AI variants like Machine Learning (ML) and Deep Learning (DL) allow machines to perform a task without human involvement, using data to learn overtime by itself rather than acting on a specific human command.[xlii] There are reports that show that ML in cybersecurity has enabled security programmers to write functions autonomously.[xliii], [xliv]

Technology Determinists would argue that with the ability of ML and DL to autonomously write functions, there isn't any need for a human as the machines would be capable enough to write algorithms, iterate them over time and provide strategic insights. For instance, consider the use case of DevSecOps, an approach to implement security by design within the software development and operations of an organisation.[xlv] There are increasing cases of using automation in the DevSecOps approach. This is enabling the security professionals to reduce the security review time of threat identification.[xlvi] The machines detect a privacy breach autonomously, send alerts and learn from their mistakes.

The Social Constructivists on the other end would argue that even if ML and DL can automate functions, and provide useful insights, it is far from enough. To automate a function too, you need a human to develop an algorithm that could

enable ML/DL to do so. Even if not developing the algorithm from scratch and using AutoML which allow programmers to automate the selection of algorithms[xlvii], it would still need a human to verify the algorithm selected. Also, ML/DL systems are only as smart as the data provided to them. In many situations, the data that is available is not clean and or does not have the right format to be used by an ML/DL algorithm. A human is needed to clean the data, apply labels to it and structure it in the way that can be used by the algorithm.[xlviii] Even in case of AI enabled DevSecOps that learn from their mistakes and prior examples, humans would be needed to train them. Human monitoring allows for the detection of any corruption of the datasets. It helps to test whether the conclusions produced are correct, and guarantee compliance.[xlix]

Automated cyber-attacks

Automated cyber-attacks are increasingly being used by hackers. They help them to increase the scale of their attacks and generate more profit in an efficient manner.[l] Types of automated cyberattacks include credential stuffing that uses previously stolen passwords to break into the online accounts or hacker bots and malicious chatbots.[li] A recent example of an automated cyberattack includes Dunkin Donuts' DD Perks program in which the hackers used credential stuffing to access the profiles and personal data of the owners of DD Perks rewards accounts.[lii]

Technology Determinists would argue that there is a need for fully automated cybersecurity systems to tackle the high scale of automated cyber-attacks. According to a 2019 report by Capgemini on AI and cybersecurity, 69% of the enterprise executives surveyed felt that AI would be essential for responding to cyber threats and filling in the existing cybersecurity skills gap.[liii] On the other hand, the Social Constructivists would argue that if there is a shortage in cybersecurity skills, that shows the need for industry and government to invest in training people. Afterall, the capability of the automated machines also depends upon the training and knowledge of the humans who wrote their algorithms.

Environmental

Militant motives

While the environmental impact of a privacy breach might not cross our minds at the first go, it can be much more disastrous than a financial breach. For instance, in 2015, cyber attackers infiltrated the network of a German steel mill, hacking into the production control system and manipulating the blast furnace to not shut down. The incident led to significant property and environmental damage. Such cyber-attacks could be very dangerous as their incentives are expected to be ideological, political, and militant.[liv]

Technology Determinists would insist that the cybersecurity of the environment industry should be completely automated, looking at the scale of potential damage to mankind. The Social Constructivists on the other hand would argue that it is going to be humans who will bear the brunt of any environmental threat and not the machines. Thus, they would be the most incentivised to avoid such cyber-attacks from happening.

Analysis

The above debates lay out the binaries on key issues and debates of privacy breach in cybersecurity systems with or without the application of the HITL model. The reality, however, lies somewhere in the middle and this section attempts to bring it to the fore.

Philosophical, ethical, and social

Social and ethical value of automated cybersecurity systems exists only because humans exist. Without the threat of any theft, people have a greater chance of living their lives in peace and happiness. Humans understand the value of privacy the best and would be best placed to prevent its breach. Theoretically it might seem that full automation of

cybersecurity systems would avoid any humans from being able to access valuable data. However, this is not possible as most automated algorithms are still dependent on humans. Also, not having humans within the cybersecurity loop might make it easier for hackers to manipulate the system because of lack of human monitoring.

Humans do make mistakes but tagging them as the weakest link would be unfair. The reason is that humans still control most of the security systems, monitor valuable data, use vulnerable machines and software. Therefore, they are the natural key to any privacy breach. It is equally likely that machines might replace humans as the weakest link if in future they are put in complete control of critical security gateways. Be it human or the machine, the one who is at the frontline will take the blame. In fact, with the coming in of IoT enabled devices and companies moving their infrastructure to cloud, the scale and reach of cyberattacks has increased multi-fold. Therefore, it might be much easier to hack into the machines than manipulate humans, especially when there is no human to keep an eye on the systems.

While humans make mistakes, they also possibly avoid making many more mistakes by using their intuitive ability to make judgements. Human judgement is critical to avoid privacy breaches from happening. Whistle blower examples discussed in the previous section make this point. Despite the Big Data revolution, data only exists for things that have happened in the past or are happening now. Thus, it would not be directly applicable in a new or future scenario. Projections based on existing data have their limitations. This is where human judgement becomes critical as it allows one to make important decisions with limited data available.[lv]

Political

On the question about transparency while there is truth in machines not understanding the innate value of data, this argument overlooks the fact that this same ignorance of a machine makes it prone to hacks. While some humans can be manipulated, there are many who are morally upright and cannot be. However, in case of machines, all of them can be hacked. This is a departure from some traditional development economic thinking according to which technology enhances transparency in the functioning of the organisations.[lvi],[lvii] While this was true for technologies like the internet, whose function was to provide humans with quick access and visibility to information, it is not the same for AI. This is because AI assists humans by automating some of their tasks and therefore essentially takes the human visibility away from those automated tasks. Thus, human involvement would enhance visibility and in turn transparency of the process. This is critical for both public and political acceptance.

On accountability, it would be fair to say that the onus ultimately lies with the human being. However, there is not one specific human that needs to be blamed. It is the collective responsibility of the software developer who designed the product, company professionals or individuals who demand that product while ignoring its security standards and the politicians who did not have the right policy or guidance in place. There might be something to learn from the aviation industry that uses the concept of organisational liability and not individual liability. For example, in a case of air-crash investigation, emphasis is not on apportioning blame, but seeking to improve the process.[lviii]Also, it is unfair to hold a human responsible if he or she is not fully involved in the process but is in there only as a rubber stamp to bypass regulatory scrutiny, like the right to explanation within GDPR as discussed in the previous section. Therefore, human accountability should be underpinned by human agency.

Also, it is critical to understand that privacy breaches arise out of both human mistakes and wrong intentions. Thus, it is a behavioural problem too. Hence, we need more humans in the loop to keep an eye on each other and monitor our behaviour rather than take them out of the loop. This is also the logic of the distributed ledger technologies like the

blockchain. As all the transactions in the block chain are visible to everyone, it increases accountability by keeping a system of checks and balances and reduces the chances of a privacy breach.[lix]

Economic and Technological

Automated cyber-attacks, cost implications, gap in cybersecurity skills and complicated and arduous security processes make the case for automated cybersecurity systems. However, more emphasis needs to be on training the employees with the best practices in cybersecurity. This is because in most breaches the human being is targeted as the easy key to accomplish the theft. Therefore, if humans have the right training, they would be expected to not fall privy to the tricks of the hackers and most breaches could be mitigated. According to some reports, 19 out of 20 privacy breaches can be avoided if employees have the right cybersecurity training.[lx] Also, not just the firms, the government should also play a role in emphasising cybersecurity training for businesses and consumers at large.

While large scale threat from automated cyber-attacks makes a case for some degree of automation in the cybersecurity systems. However, the results of automation would be optimal with human involvement. This is because ML/DL based automation of cybersecurity systems is only as good as the algorithm behind them which needs to be developed by a human. Even if algorithm selection is automated, it needs to be verified and checked by a human before it can be fed into the system. Moreover, ML/DL operate on data inputs. Most of the times the data that is available is skewed and non-structured. Therefore, humans need to clean, tag, and structure the data before it can be fed into the ML/DL algorithm.[lxi] Also, unlike humans ML/DL don't have a discretionary mind and cannot apply context to a given piece of data. Therefore, they cannot distinguish between accurate and inaccurate data.[lxii] This is often misused by the hackers who feed them with wrong data inputs, manipulating the cybersecurity systems.

Additionally, while humans are creative beings and automating cybersecurity systems can free us of performing the monotonous tasks, is it safe to keep our valuable data absolutely in the hands of the machines? Afterall, we are not only creative but also intuitive and perceptive, which makes us better placed to have a decision-making role within the cybersecurity systems. Afterall, the hacker is a human too, and they can always innovate and inflict an attack that our machines have no prior data inputs on. In such circumstances, human intuition becomes critical.

Environmental

Humans know best the havoc that an environmental disaster can have on their lives. Thus, they need to be involved as they would be the most incentivised to avoid a privacy breach with environmental consequences.

Conclusion and Recommendations

While automated cybersecurity systems are important in terms of – managing the scale of automated attacks, making the systems cost effective and saving time and energy on laborious tasks, humans still are the central players. Afterall, the ultimate value of cybersecurity systems lies in benefiting humans powered by human preference and agency. Thus, it is critical to have human involvement as they would understand best what is good for them.

However, they might not be able to perform optimally without the right training and/or education. This brings the emphasis back on the existing skills gap in the cybersecurity sector. Once trained, humans are expected to modify their actions, in turn reducing the chances of privacy breach. The nature of the training should be multidisciplinary. This is because training limited to only technological aspects would not allow individuals to fully understand the wide array of implications of a privacy breach, across various parts of the economy[lxiii] as discussed in the previous sections. This is because we live in an embedded economy which operates through active feedback loops cutting through and across different terrains of the economy.[lxiv] Therefore, if any one terrain is out of balance, others will be

impacted. Thus, to enhance the judgement of cybersecurity professionals it is crucial that they are trained in a holistic manner. They should understand the implications of their actions on consumers and society at large.

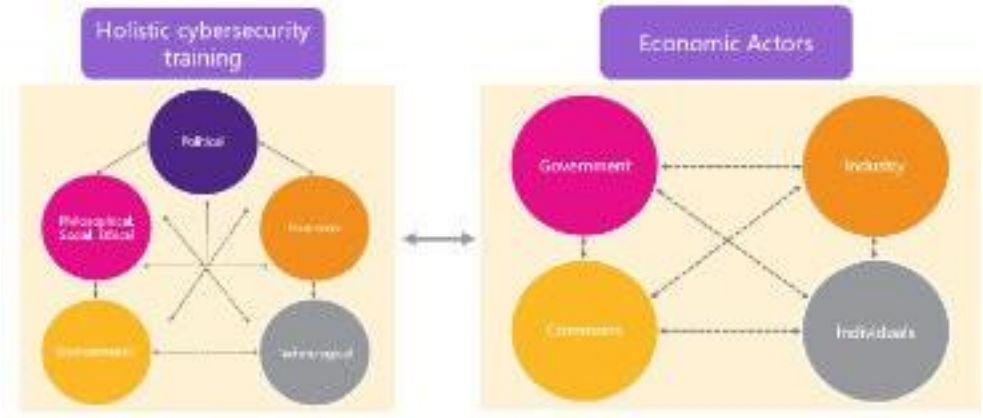
The emphasis should be on developing a holistic understanding about privacy implications of cybersecurity systems. The question is not only about the impact of having or not humans involvement but about having suitability skilled individuals who understand the intricacies of a privacy breach across the domains of society, politics, economy, technology and environment. This holistic understanding should then underpin clear policy and regulation on automation of cybersecurity systems. All economic actors have a role to play in this i.e. the government, industry, commons[lxv], and consumers.

Industry should realise the onus of social responsibility that they hold now. People have entrusted them with their personal, financial, and business-related data, which in the past was either vested with the government or with the individuals themselves. Therefore, industry professionals should actively invest in training their employees in cybersecurity best practices. Emphasis should be to hire multi-disciplinary teams.

The reach and creativity of the commons should be harnessed. This includes both consuming and spreading awareness using online blogs, youtube videos, open source data and learning platforms. All economic actors can benefit from commons, however some caution would need to be paid to the authenticity of the source of the information.

Consumer demand is the driver of supply. The challenge however is that consumers are usually not aware of the backdrop complexity of the products and services they consume. Consumers should utilise the power of the commons to enhance their understanding about automated cybersecurity systems and its privacy implications. Only if they understand, will they ask for the involvement of greater human involvement and that too suitably skilled people with agency and well-rounded understanding of the issues. Without consumer engagement, we do not really have public acceptance, rather only ignorance. Figure 2 below illustrates the proposed way forward.

Figure 2: Need for multi-disciplinary cybersecurity training and engagement between all economic actors[lxvi]



References