*International Journal of Engineering & Technology,* 7 (2.34) (2018) 93-97

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*

***Research paper***

# ICT advancements and its undesired ramifications

**Abdul Haseeb Ansari ***

*Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia, Malaysia*
**Corresponding author E-mail: ahaseeb@iium.edu.my*

**Abstract**

Information and communication technology (ICT) has the credit to be relatively more closely related to the society facilitating economic transactions to be easy and fast and social wellbeing in all walks of life. It has had global and international importance, as it has worked as an important tool in globalizing the world, and has become a pressing necessity of the globalized world. Moreover, its relevance in the globalized world is intensifying, as its constructive role is every day spiraling. Its vale in that sense will go on mounting. On the other hand, its evil-ridden uses and abuses are menacing the people and countries around the world. Delinquent people and rogue countries are using the technology for achieving their sinister objectives. This aspect of the technology is bothering policymakers, business executives and individuals in the society. In view of this, two pertinent questions arise: one, which of the two aspects of the information and communication technology is dominant; and second, what preventive and punitive measures should we adopt in order to mitigate the evil use of the technology. A vivid comparison of both, which has been carried out in the paper, demonstrates that the beneficial use of the information and communication technology is predominantly high. Thus, our strategy, as the paper suggests, should be to support the useful aspect of the technology with useful conditionality so that it could abate and control its evil use, and to adopt preventive and punitive measures in order to defeat the evil-doers. For that, both legal and extralegal tools should be adhered to. Towards these, the paper offers some useful suggestions.

## 1. Introduction

Socio-economic use of information and communication technology is immense and spiraling in the contemporary world. Some significant ones are discussed below.

## 2. Some day-to-day use

### 2.1. Democratic endeavours

Any act at any level democratically done, garners support and serves the best interests of all participants. May it be a social organization, a business organization or a political organization, democratic process is considered to be amicable. But before a person goes on to participate in any decision-making he should have enough relevant information [1]. Both the dissemination of information and participation subsequent to that, have been made easy by the manifest use of information and communication technology. The best example of using ICT in holding general elections is there in India. It is notable that the whole election process, from voting to counting of votes, is completed by application this technology. The ballot paper is displayed on a monitor. The voter simply touches the symbol or the name or photo of the candidate of his choice, his vote is recorded in the database, and the system automatically closes. For the next voter, the returning officer has to on the system again, and the process goes on until the voting time ends or the voting is complete. Counting afterwards on the day of counting does not take much time, since all the votes are already there in the database; only problem cases are looked into and decided on. It eliminates all kinds of possibilities of rigging and phantom voting, which were common before.

### 2.2. Trust in the government

Good governance is crucial rather sine qua non for any form of government - kingship, dictatorship, aristocracy, presidential form of democracy like that of the United States, Westminster form of democracy like UK, Islamic form of democracy (Khaflifa and Shura), or unitary or federal form of government – to be in the public interest and in the interest of the state. Good governance of a state, especially of a democratic state, commands trust of its people, because trust of its people makes it a popular government; and constitutionalism demands an unpopular government has no right to stay in power. In order to continue to maintain trust of its people, states: should have to release relevant information, other than information marked as confidential, to the people; should have to invite public participation; and should provide easy and efficient access to justice. In order to be genuine the three aspects of good governance must be practiced honestly with total transparency and accuracy of information. These three cardinal points of good governance are considered to be crucial and are being practiced at national and international levels to strengthen the imperatives of informed decision-making and ensuring constructive public participation. The best example of this is decision-making in environmental matters. The Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters, 1998 (Commonly known as Aarhus Concatenation) of Europe is a known international legal document, which has been wholeheartedly internalized by European countries. Its tenets are being practices at state level also. The best example of it at the state level is the Malaysian law on making environment impact assessment (EIA) enshrined in the Environmental Quality Act 1974 and the Environmental Quality (Prescribed Activities) (Environmental Impact Assessment) Order 1987 read with EIA Guidelines. They together prescribe for input of public participation before a project is allowed

to go ahead [2]. Same goes with the relationship between government departments, companies, corporations, and NGOs. Wherever necessary, the three elements given above should be practiced for ensuring good governance. Good governance also plays a vital role in garnering support of foreign investors. Before they invest, they want to know the economic indices of the country because they wish to assure that their investment is going to be productive. In the whole course, accuracy of information by easy access to informational by technological means is central because it works in confidence building.

### 2.3. Prevention of corruption

Corruption is antagonistic to good governance. In most of the countries they go together but adversely impacting each other. Good governance requires fairness on the part of the every participating person. However, ICT has helped strengthen good governance and has worked for alleviating corruption. When information is on line or in database, hardly anyone would dare to breach the system and practice corruption because most of the databases do not provide chance of manipulations as almost all of them are protected by one or the other security mechanism(s). There was a time when all land matters in land departments of almost all countries were maintained manually. This provided chances to people dealing with ownership and mutation in ownership registers to practice manipulation. Likewise, land frauds also flourished mainly by way of misrepresenting the owners while selling properties and changing the nature of the land, viz. from graveyard to settlement. When each and every relevant information went online and became part of the databases of the land department, these kinds of land frauds became uneasy to be practiced. It can only be practiced if there is connivance or conspiracy of all concerned officials. Moreover, transfer mechanisms are fortified with certain procedural requirements and which are electronically preserved. In addition to that, any corruption incident can easy be made viral on social media, which tarnishes the reputation of the official concerned. It works as a high degree of deterrence to other people. The other example is keeping the whole tax-system online. From return filing to assessment to re-assessment and imposing fine and recovery and refund are online now. It provides least opportunities to the tax officials and taxpayers to meet. If they do not meet, almost all personal whips and whims are eliminated; dealings are no more tainted of corruptions.

### 2.4. Allowing tracking of transactions

An efficient tracking of all social, communicational and commercial transactions is a boon appended to information and communication technology. A letter if posted can be tracked until it reaches the designate person. Likewise, one can check his summons online within seconds. Moreover, if anyone has committed a fraud which is detected after the payment online has been made the payment can be stopped at all payment systems. In the same way, an offer can be tracked until it is accepted.

### 2.5. Publicity

Now, publicity of anything and everything depends on information and communication technology. All services and products can be easily and aptly publicized by the use of mass media and social network. For example, during general elections, political parties do much not believe in organizing public speeches. They prefer to approach their voters through my electronic means and mass media. They are easy, accurate, prompt and effective. In the United States, presidential elections mainly depend on debates between the representatives of the two prominent parties and people watch the debate on televisions/phones or any other electronic gadgets, and read in newspapers. In fact, publicity has become a tool to promote persons or properties and ideas.

### 2.6. Teaching and learning

ICT has provided immense facilities with flairs to teaching and learning and pursuing researches. Online reading materials and distant learning have brought them to the doorsteps of indigent people. They now can have access to reading research materials on least expenses or for free with minimum of efforts. There are service providers which are generally subscribed by institutions of higher learning for the benefit of their students. Other than that there are a large number of journals and books accessible online for free. Likewise, all statutes in the form of primary and secondary legislations, and decided cases from all over the world are online and freely accessible. Similarly, there are systems to provide teachers and students to interact without physical meetings. This is possible through a website especially designed for this purpose, viz. the International Islamic University Malaysia (IIUM), Malaysia has i-ta'leemk, which is easily accessible by lecturers and students. Uploading materials for students, uploading assignments by the students, and questions and answers are easily carried out through this. In fact, all events from admission until graduation are now online. This has made the education system, fast, efficient and motivating.

We have discussed above some of the beneficial uses of the information and communication technology. These compounded with some others warrant that computer literacy in general and insight in the means of communication has to be a matter of priority so that the use of ICT could be maximized. For that, the lucrative Malaysian program of 'one family one computer' is quite appreciable. India also has similar scheme. These with ever-growing use of mobile phones will certainly yield appreciable results. The urban people are already conversant and are making use of them. Rural mass requires special attention in these matters. For an efficient use of ICT, a proficient networking is required; in fact an easy and fast networking service is the only solution. There are a large number of service providers, but all of them require am swift Wi-Fi. Only this will ensure easy accessibility, usability and functionality; they have to be best user-friendly. Every day, commercial and social and other transactions are going online. In view of this, these imperatives become a matter of priority of the governments, central, states and municipal corporation level.

## 3. Personal data protection

Privacy is a condition of life characterized by exclusion of publicity. It is exclusively relates to a person or class of persons as the case may be. Personal data, especially genetic traits, physiological infirmities, personal relationship data and criminal engagements, of an individual are personal to him. Others, thus, as a matter of rule, are bound to maintain privacy about them; otherwise, the person, who divulges them, may be liable, which might be even criminal in nature. However, personal data can be released within the scope of law in the greater interest of the person concerned, or by order of a court or in public interest with or without permission of the person concerned or a competent person if the person is suffering from some kind of disability. The whole gamut of legal rules and popular practice depend on personal interest on one side and public interest on the other side. Since both the aspects are equally important, formulating a balanced law is a difficult task. However, there are some clear cases where public interest can be given precedence over privet interest. For example DNA database are maintained and used by the police department in public interest for prevention, abatement and control of crimes even without permissions of perpetrators [3].The author is of the opinion that with respect to protection of personal data, a meaningful balance between private interests and public interests should be maintained. Personal data are now stored electronically and carried from one place to another place on CDs or sent through secured social media. Most of the places have it online. Any concerned person authorized to access can look into it. The best example of that is paperless hospital. All the details about patients are there online. Any amortized person can look into them just by entering a password. It has been reported in several cases that criminal and medical data have been divulged by the authorized person or hackers. In view of this, it is suggested that such systems

of personal data should be infallible and protected by an efficient security system.

## 4. Promotion of E-commerce

The maximum use of ICT is there in business and commerce. It starts with online advertisements, all kinds of commercial transactions viz. sale, purchase, distribution, supply, hire purchase, mortgage and lease have antecedent contracts, and thus are governed by the general rules pertaining to formation of contracts. Detailed rules are there in specific legislations. Both go hand-in-hand. Use of ICT for entering into contracts has made the process fast. But entering into contracts by electronic means using social networks is not a smooth sailing. It gives rise to a number of legal questions, which may give rise to intricate legal issues: Is the offer deceptive? Are the parties major? Is the financial conditions of the promissor is sound? Is there any misrepresentation or fraud? Is the material sought to be purchased or a job is sought to be done are genuine and within the purview of the law? Have the conditions and warrantees, statutory and contractual, appended to sale of goods been complied with? On the top of these, if the buyer is in one country, the seller is in another country and the goods upon sale and the price have to move from a third country to a fourth country, the decisions on – as to where the contract has taken place and in case of any legal dispute which country has the jurisdiction to try the case - are intricate legal issues. Likewise, the question to decide as to which country is entitled to impose indirect tax on the transaction and where the income tax will be payable further complicate the issues. Transfer of money for whatever reasons one country to another country- via bank to bank, through moneygram and other such means - has become very easy and fast. But they also pose legal questions in certain situations.

In order to comply with the laws and avoid possible adverse legal consequences, first and the foremost requirement is to avoid deceptive advertisements in the media or on the net. The disclosure of the products or product information should be within the legally prescribed limit. Proper heed should be given to the conditions and warrantees, statutory and contractual, and promises should be kept. It is necessary to judge the deceptive advertisement and methods of verifications should properly be invoked. The liability for ill-judging cannot be fixed on the other party. It is better to know in advance about all possible legal and extra-legal implications of online trade.

## 5. Ill effects

ICT has opened numerous avenues of committing cybercrimes. They are running parallel to the beneficial use of the technology and are afflicting the society. There are over 4 thousand attacks every day. According to the IOBM estimates, business are attacked an average of 16,856 times a year. Although it is difficult to estimate exact figure of loss due to cybercrimes, Mcafee estimates that the annual global cost of various such crimes is about 400 billion dollars [4]. It can reach to 575 billion dollars [5]. It is expected that the situation is going to be intense with the increase of the use of ICT especially for business and increase in the organized cybercrimes. Cyber criminals take full advantage of the anonymity, secrecy and interconnectedness provided by the Internet, therefore, attacking the very foundation of the information system. One study estimated that by 2019 cybercrime loss would rise over 2 trillion dollars by 2019 [6].

In 2016, some notable trends of cybercrimes are: shifting the focus of organized cybercrimes to business; mobile threat has see mark increase in fraud capabilities; cyber extortion is at rise; card fraud shifted to card-not-present (CPN) fraud [7]. Cyber terrorism is even much more serious criminal endeavor affecting relatively larger number of people and causing serious widespread and long-term damage to the people and their economies. Both pose a serious ever-growing global problem in the world and posing even more serious security and economic problems. Keeping this in mind, security system is being given greater attention so that criminals could not have easy access to the networking. But the irony is that such criminals always go ahead of the security system [8].

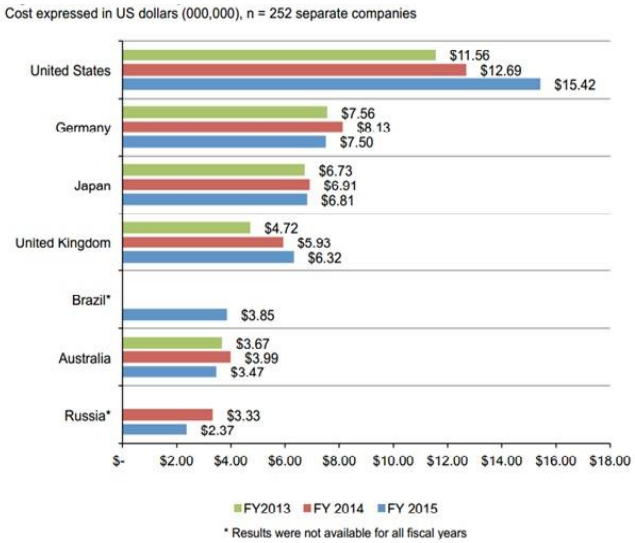


**Fig. 1:** Total cost of cyber-crime in seven countries

There is a long list of cybercrimes. Some of them, which are commonly being practiced, are: 1. Identity theft, which is actually a type of misrepresentation. It is a serious problem causing widespread damage. 2. Spreading malicious software codes, such as computer viruses. There are antivirus software(s) updated from time to time. But cyber criminals always manage to invent new viruses. 3. Hacking into other peoples' email account and sending spam emails messages, which sometimes is difficult to falsify. This warrants inconvenience of frequently changing the password, which in certain situations is not easy. 4. Hacking the network is a common cyber crime. Hackers can cause any amount of damage by manipulating the data or replacing the original data with a fake one. 5. Cyberstalking is causing harassment by using electronic communication like email or instant messaging or messages posted on a website or a discussion group. They take the advantage of the anonymity afforded to Internet to allow them to stalk their victims without being detected. This is causing relative more and serious damage to young ICT users. Because of this, lots of youngsters are coming suicide [9]. 6. Cyberbullying is similar to cyberstalking. It is an act of bully via electronic social media. This may go to the extent of blackmailing and claiming extortion upon kidnapping. 7. Cyber pornography is quite prevalent among people of all age groups, but it makes mainly teenage boys addict which adversely affects their social life and education. 8. Internet gambling is yet another cyber-crime of very high magnitude.

All cyber-crimes, including cyber terrorism, based on their nature can be put into four categories:

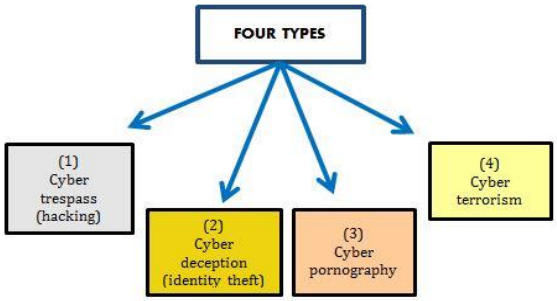


**Fig. 2:** Four categories of cyber-crimes

The other mode of classification is: 1. Where computers are targeted, e.g. hacking, malicious code, vandalism. 2. Where computers are used as a tool, e.g. fraud, theft, stalking, extortion, fraud and pornography. 3. Where computers are simply involved, e.g. use of computer to record illegalities.

## 6. Law and enforcements

Cyber crimes have their peculiar nature different than traditional crimes. They can be committed without any physical presence and disclosure of identity or contacts; they come all of a sudden, there is no prior indication(s); one person can cause damage to many computer users or even the whole operating system; and by the time enforcement authorities take cognizance of the crime, criminal(s) wrap up and run away; and most of the times, criminals are well-trained [10]. The ever-growing trend of cyber laws, which are there in place in almost all countries for quite some time and are being amended from time to time in order to make them meet the contemporary challenges, demonstrates that cyber laws fall short of total enforcement. In UK for example, there has been a number of legislations covering various kinds of cyber crimes and they have been amended from time to time. In March 2015, a new legislation named the Serious Crimes Act 2015 has been put in place with wider net of crimes and severe penalties for them. It is operative with the Computer Misuse Act 1990, amended from time to time, and the Wireless Telegraphy Act 2016. These Acts go even beyond the British territory in order to nab the crimes. Also, they are in line with the international law contained in the Budapest Convention on Cyber Crimes, 2001. These with some other legislations are competent to deal with a vast variety of cyber crimes, yet total success seems to be far. It proves that punitive measures alone cannot successfully meet the challenges posed by cyber criminals. Some cyber crimes are organized for achieving mainly any political objectives; some are committed by individuals for accomplishing individual interest; some others are committed for fun or in sports. They have to be dealt with separately by a competent and sufficiently trained staff so that the problem of tracking could be strengthened. There might be lack of consciousness on the part of persons who are commuting the crimes. There might to need to train general public using ICT to observe a computer security system, and use latest operating system.

## 7. Defamation: A dilemma in ICT

There is an ongoing debate on legal significance of statements posted on social media. The freedom lobby holds the view that in view of the increasing support for freedom of speech, especially in democratic countries, and expression everything written on any social media should be out of any legal action even if it is unsophisticated or defamatory. On the other hand, lots of people are in favour of this kind of absolute freedom; they want legal actions be taken against all kinds of libel on social media. In India, section 66A of the Information Act 2000 authorized the police to arrest people who committed libel by writing something considered as libel, with whatever motive, on social media or who liked any such writing. Almost all actions taken in form of arrests taken by the police became subject matter of criticism on the ground that criminalizing such acts violated the freedom of speech and expression guaranteed under the Constitution of India. In March 2015, in Shreya Singhal v. Union of India (Writ Petition No. 167 of 2012), the Supreme Court of India ruled that section 66A was unconstitutional. It means, there cannot be any criminal action against any libel published in any social media. It is clear from this case that there cannot be any criminal action against any defamatory statement posted on any social media. However, there can be a civil suit against such a statement and the liability to pay damages can be fixed by the court if the statement is determined to have caused damage to the complainant (Plaintiff). It is to be noted here that generally speaking, a statement of facts does not amount to defamation. An opinion may or may not be defamatory; if court determines it to be defamatory there will be a liability to pay damages. Modification of photos or any pictures or statement making it insulting or defamatory will also be actionable [11]. Here a legal question arises as to whether the service provider of the social media is also liable for it. The answer to this will depend on the law. In the United States, the service providers have been exonerated under the Communications Decency Act 2005 from any liability for any posting by any user.

## 8. Conclusion

The paper has shed lights on both the aspects of ICT, beneficial and disadvantageous. But the beneficial use has surpassed the harmful use. However, it is a known fact that those who are using Oracle Java, Adobe reader or Adobe Flash are at high risk. They together constitute 99 percent of all computer users. It is also known that malicious insiders, mainly from employees, steal 59 percent of the data. Social engineering - which in the context of information security refers to psychological manipulation of people into performing actions or divulging confidential information, and which is a confidence trick for the purpose of information gathering - is the common way of manipulating victims. It is accountable for the $ 1 billion loss in 2 years involving 100-banks of 30 countries. There are cases where government is blamed for practicing malware. The irony is that some of the cybercrimes, especially related to cyberwar, state secrets, military secrets, and industrial espionage, are practiced with governments' support. Almost half of the cyber attacks are motivated by hacktivism, which a subversive use of computers and computer networks to promote a political agenda. With roots in hacker culture and hacker ethics, its ends are often related to free speech, human rights, or freedom of information. 78 percent of lost funds due to cyber attacks were unrecoverable [12].

In view of these, it is warranted that in the interest of states and their people, all states should have a viable policy on augmenting the research and best use of ICT products. The policy should be based on the following strategies: to improve customer experience of government services; to work for digitalizing the economy; to have an efficient information management; to keep relevant data to be accessible by the stakeholders; to maintain information security and privacy of individuals; to have digital achieving; to work for contestability and ICT strategic sourcing; to work for having a capable workforce; and to develop optimum competency with respect to portfolio, program, and project management competency. The overall goal of the policy and strategies designed under it should be able to provide safe and secured ICT services with saving of time and money. There have to be two key-elements to build on, efficiency and security. Only then there will be the following desired results:

- The Public Service will be more agile and deliver more user centric and innovative services for citizens and businesses.
- Innovative use of ICT in the Public Service will deliver better value for taxpayers by creating efficiencies through integration, consolidation and sharing of common infrastructure, systems and resources.
- Adoption and facilitation of digital technologies will increase productivity, improve the relationship between citizens, businesses and government and will deliver social and economic benefits for Ireland.
- Integrated services and increased data sharing will drive significant efficiencies; will facilitate insight driven decision making; will increase openness and transparency between Government and the public; and will provide a much higher user experience and quality of service for citizens, businesses and public servants.
- Improved ICT governance will ensure alignment, reduce risk and support unification as envisaged under the Public Service Reform Plan and Civil Service Renewal Plan.
- The future needs for ICT skills will be met through professionalization of ICT streams, targeted recruitment and improved mobility and succession planning across all public bodies [13-15].

Governments, companies and corporations should also constantly work on making the concerned officials and technocrats competent to face the challenges by the evil-minded people who work for sab-

otaging and/or steeling data or identity theft. Their R&D departments should continuously tell the people and persons specifically concerned to practice strategies to block hackers.

## References


[1] Abdul Haseeb Ansari, "Principle 10, Aarhus Convention and Status of Public Participation in Environmental Matters in the Malaysian Laws with Special Reference to EIAs", IIU Law Journal, vol. 17 Number 1, 2009, p. 57.

[2] Ibid

[3] "Personal Data Protection" at: http://www.echr.coe.int/Documents/FS_Data_ENG.pdf (Accessed on 12 September 2016).

[4] "These Cybercrimes Statistics Will Make You Think Twice About Your Password: Where is The CSI Cyber team when you need them?", at: http://www.cbs.com/shows/csi-cyber/news/1003888/these-cyber-crime-statistics-will-make-you-think-twice-about-your-password-where-s-the-csi-cyber-team-when-you-need-them-/ (Accessed on 12 September 2016)

[5] Center for Strategic and International Studies, "Net Losses: Estimating the Global Cost of Cybercrimes", 2014, at: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf 9Accessed on 20 September 2016).

[6] Steve Morgan, "Cybercrime Cost Projected to Reach $2 Trillion by 2019", at: http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#a1d0b7d3bb0c (Accessed on 12 July 2016).

[7] "2016 Cybercrime Re4load: Our Predictions for the Year Ahead", at: https://securityintelligence.com/2016-cybercrime-reloaded-our-predictions-for-the-year-ahead/ (Accessed on 12 July 2016).

[8] Computer Crime Research Centre, A. Snhetlor, "Some Problem of Cybercrime and Cyber Terrorism fighting" , at: http://www.crime-research.org/library/Schetilov.htm (Accessed on 13 June 2016).

[9] The National Centers of Victims of Crimes, Bulletins for Teens Stalking, at: http://victimsofcrime.org/help-for-crime-victims/get-help-bulletins-for-crime-victims/bulletins-for-teens/stalking (accessed on 12.10 2016).

[10] RAS Conference, "Cybercrime and Effective Cyber Law Enforcement", at: :https://www.rsaconference.com/blogs/cybercrime-and-effective-cyber-law-enforcement (Accessed on 10 July 2016).

[11] Find Law, "defamation and Social Media: What You Need To Know", at: http://injury.findlaw.com/torts-and-personal-injuries/defamation-and-social-media--what-you-need-to-know.html (accessed on 17 September 2016).

[12] "10 Alarming Cyber Security Facts the Threaten Your Data (updated on 12 May 2016)", at: https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/ (Accessed on 20 July 2016).

[13] "Public Service ICT Strategy", January 2015 at: http://ictstrategy.per.gov.ie/ictstrategy/files/Public%20Service%20ICT%20Strategy.pdf (Accessed on 20 AUGUST2016).

[14] Ahmed, S. F. (2007, December). A new approach in Industrial automation application" Embedded system design for Injection Molding Machine". In Multitopic Conference, 2007. INMIC 2007. IEEE International (pp. 1-5). IEEE

[15] Ahmed, S. F., Kushsairy, K., Bakar, M. I. A., Hazry, D., & Joyo, M. K. (2015, April). Attitude stabilization of Quad-rotor (UAV) system using Fuzzy PID controller (an experimental test). In Computing Technology and Information Management (ICCTIM), 2015 Second International Conference on (pp. 99-104). IEEE.