The Eighth International Conference on Business Information Security (BISEC-2016), 15th October 2016, Belgrade, Serbia

INTERNET OF THINGS CHALLENGES FOR ORGANIZED SOCIETIES

MIROSLAV D. STEVANOVIĆ
Security Information Agency, Belgrade, mstvnv297@gmail.com

DRAGAN Ž. DJURDJEVIĆ
Academy of national security, Belgrade, djurdjevic.dragan@gmail.com

Abstract: *The concept of the Internet of Things (IoT) implies consequent interconnectedness of humans, devices, equipment, and maybe even wildlife. In the process of spreading of IoT, societies become more complex, and thus exposed to new challenges for their stability. The problem, from the anthropocentric aspect, is how the concept of the IoT affects an organised society. We assume that the public administration has an institutionalised duty to prevent security breaches within its jurisdiction, and provide security of sensitive applications, including national infrastructure, security services, and the finance. In this article, we observe foreseeable challenges facing national administrations through the IoT order, and political balance. We find that information input and time consumption implied by the IoT will immanently affect decision making, that omnipresent infrastructure environment will broaden legal and national security issues of the State, and that interconnection introduces a concept of conflict in social life. The results indicate that to maintain social stability, States faced the necessity of preemptive action in the sense of creating educational, legal and technological preconditions for a new stage of technological change.*

Keywords: *IoT, Infrastructure Environment, Sustainability, Information Management, Human Rights*

1. INTRODUCTION

In the process of spreading of IoT, societies become exposed to new sensitive applications, including national infrastructure, security services, and the finance challenges for their stability.

In our previous articles concerning matters of national and public security challenges of spontaneous spreading of application and development of IoT, we have indicated a number of obstacles facing public authorities in regard to the interests of individuals. These obstacles are concerned with the problems of providing the functioning of networks, clouds, network security, or advances in a rational deployment of independently communicating sensors and appliances [1].

The approach which exposes only the responsibilities of public administration as a regulation of technological standards on the territory necessarily deprives a society of an organisational component.

The global network is not an artificial intelligence and, in the functional sense, it is just a tool through which mankind enhances its potentials. Structurally, it is unavoidable that widespread of "smart" sensors and applications will influence processes in various fields of human life. What is basically at stake is the stability of legal order, and political balance in changing societal arrangements, in which sensors have an independent influence on the decision-making process.

Questions arising from IoT concept exceed the comprehension of its functioning, and even potential misuse. They epistemologically root from dilemma is it possible to uncritically implement a complex system of interconnected and communicating sensors in a way that would improve and not marginalise human rational efforts.

2. MATTER OF NATIONAL LEGAL ORDER

Internet of things includes the aspect of popular trust. Ethical framework of that trust creates a responsibility for public authorities of a country, as a consensually developed dominant organisational form in a political community, to publicise desired norms and to incorporate them in the framework of trust. Thus, the first obstacle is of epistemological nature, and concerns approaching the new revolutionary technology since the knowledge itself is simultaneously social and technological phenomenon.

Ethical trust in new possibilities of IoT necessitates the dedication of public authorities to present all perceivable frameworks [2]. There is little room for doubt that power of automatized computing will affect the everyday life. The fact that, due to that, society's environment can become better or worse, is the essence of the IoT. Independent objects become as they are functionally represented on the network: monitors, controllers etc. Having communication with objects, in new roles, necessitates a change in the philosophical paradigm of normative order, in terms that it has to include new mutual interrelations between prior subjects and objects. The consequences of the paradigm shift can already be conceptualised in many activities, automatized habitats, organised care of elders, children, life in cities etc. But, an organised society cannot effectively function if the normative intrusion is not in line with prior, more general norm, and that is subject to an ethical framework [3].

Conceptual implementation of IoT is still far from a full and necessary connection of all services and technologies. From that aspect, the question of new philosophical-

normative paradigm may seem premature, since today we are faced more with a variety of solutions and efforts aimed at ensuring The semantics of this orientation of IoT prioritises management of an as wide spectrum of services as possible [4] regardless of the normative requirements.

Normative ground for the functioning of IoT, apart from resolving the mentioned ethic dilemma, what is good and what is wrong in individual and collective behaviour, for the society, has to include an axiological aspect, namely a new aesthetic concept which will be imposed through the implementation of IoT [5].

The principle problem which organised societies encounter in all matters concerning the internet is that national law ends on national borders, and no individual state has exclusive jurisdiction over the internet, and especially not the IoT.

Public administrations perform many functions provided by the law. Some Cyber systems have the potential to optimise the use of processing and storing resources, like virtualization (abstracting applications from the hardware) or cloud technologies (based on virtualization), and enable sharing between various administrative entities [6]. Hosting of resources of public authorities on clouds outside institutional and democratic control poses a challenge for the protection of individual and collective values.

Apart from the institutional and democratic issue, organised communities are facing a challenge generated by the prompt availability of surrounding, which introduces IoT. Cloud computing is graded, flexible and omnipresent, with use almost everywhere, science, health care, economy and everyday life" [7]. Having in mind a projected sharp rise in quantity and volume of interconnected networks, the matter of norming safety and privacy cannot be left for ex post regulation. The prospect of connecting virtually everyone and everything inevitably has to affect basic communication norms of today, which are human-centric in a way which is impossible to anticipate. In the mentioned context, of service orientated network architecture, a challenge for nation states stems from the fact that artificial "intelligence" enables solving some specific problems, i.e. decision making, through physical and virtual entities fulfilling autonomous goals, which is an additional risk for public affairs, as well as privacy, in certain areas, like health.

3. MATTER OF POLITICAL BALANCE

Structures of power in contemporary societies (concerning the control of capital, statics and relations between social groups) today, in the post-modern age, are simultaneously highly exploitative, unjust or oppressive, and above all generate degradation of the human environment [8]. From only the aspect of public safety and security, the threat emerging from IoT pose ever more devices coming online with new ways to exploit them and possibilities of distributed attacks. But, in the interest of functional and effective society, there are more fundamental, practical questions facing every individuals and society: what are human beings giving away; where is the data going; who will really own "our" devices in the new future; how the homes are automated, how we care for the elder, how do we monitor children, what concepts are used to organize life in cities etc. Answers to these questions are not currently a priority public concern, and producers don't have a commercial interest to explain the consequences.

From the aspect of these activities as societal arrangement, the IoT challenge extends beyond only the induction of normative elements, and can be generalized in the context of - for the benefit of whom, and for the good in accordance to what norm. Thus, this challenge is simultaneously political and ethical in nature.

The IoT will consist of perception technology embedded in physical entities, networks for exchanging the data they generate, computing power for interpreting them in real time (as a service), and finally, agents that react according to computing results. We can assume that capabilities of computing power distributed and embedded into everyday objects and the connectivity of the net will make everyday world more "intelligent". But, as devices and sensors will in many ways shift real-time connectivity to physical human body, it will have to effect social abilities in the real-world. The risk, namely, is that psychologies of confused identities and power play could cause chaos, or have some other limited negative repercussions [9].

Society will, considering the correlation in the tendency of high technologies towards investment centers, undoubtedly, generally be enabled by cheap technology [10]. Some will afford full automation, but will all, or at least most? Consequently, individuals and societies will, as a rule, be in a position to make simple commands, but not to influence complex actions together. So, the systemic functions that citizens rely on in everyday life will remain dependent on bureaucratic, but digital solutions. Integration of technologies will thus necessarily be an ongoing issue, from the aspect of purpose, and from the aspect of elitism.

There is no reason to assume, neither to doubt, that the humankind will eventually reach its potential to keep up with the "smart" machines, or even reach artificial intelligence. But, until that time there is a serious risk that IoT could lead to anonymous networks dominating the affairs and being factual caretakers. As the processes rely ever more on the digital world, even the interactions between humans may become ever more virtual.

All life has instinct value, independently of its usefulness to humans. Richness and diversity also have value in themselves, because they contribute to the well-being of life in society. If IoT should, as it seems, lead to a reduction of this richness and diversity, unless it is to satisfy vital needs in a responsible way, there is a question of a right for such alteration. Human lifestyles and population are key elements of human impact, and the diversity of life, including cultures, can flourish only if the human impact is reduced, regardless of advance of useful digital objectification in everyday life. This is why it seems inevitable that basic ideological, political, economic and technological structures must change. If we accept that there is an obligation to participate in

implementing the necessary changes that impose IoT, it must be assumed that it includes the duty to secure that they are peaceful and democratic in nature.

The impact of the IoT on society, and primarily the increased role of technology, could develop alienated automatism in many decision making processes. That is the direct purpose of many software and services that are produced and incorporated. This impact carries numerous social uncertainties, which are attributed, among others, to: generation of large quantities of generated data, which may or may not necessarily be valuable or needed, but are potential for use or misuse; privacy, data protection, and social issues opposed to the potential benefits in public safety, energy conservation, and lower costs, depend on public opinions and behavior; potentially large-scale, highly automated technological systems that can remove human intervention in order to increase reliability, but increase the potential for societal vulnerability, with uncertain inevitable higher quality in the provision of many services; and inequality in access to data of value to individuals and communities, parallel with other digital inequalities across societies [11].

But, if we consider technology to be a tool, interconnections and interoperability cannot be accepted as detrimental in decision making. That is why there is a need to consider the impact of the IoT on the wider society, and not just on organizations. Since IoT will change many social ways, crucial for its viability is organizational and institutional innovation.

4. MATTER OF INTERNATIONAL SYSTEM

Tomorrow's internet landscape could look very different: new smart systems, available on the go, new social media, cloud computing that is scalable, flexible, and everywhere, enormous data sets used in science, healthcare, economy, and everyday lives.

Networking of different technologies and domains, in building of architecture of interconnected humans and objects leads to new challenges in regard to manageability, security and privacy on the supranational level. Many fields of human activity require formal normative and political coordination of deployment and implementation of sensors at international level. Environment, chemistry, biology, radiology and the nuclear sector cannot be left to corporate technologies and services if IoT is to be trusted by populations.

Due to a large number of applications, providers and stakeholders, standards need to be adopted at international level, so that in practice IoT system would at least function as interoperable [12]. Interoperability is, as such, a specific potential risk generator for at least two reasons: firstly, due to the dissonance between management requirements and engineering concepts, on one side, as well as due to the discrepancy between the perception of decision makers and effectiveness and reliability of developed solutions. From that aspect, it seems that the current concept of security, as isolated criteria, needs adjusting, since it contains fundamental structural incompatibility with the idea of interoperability, which tends towards global inclusiveness, thus also globalizing the challenges.

The question of national and international politics concerning management of cyber sphere is already being regionalized. Cyber defense is part of NATO strategy since 2002. Within this strategy, member and partner states are offered various mechanisms of potential crisis management and strengthening of national cyber defense capabilities. This way, countries are being guided into a unified frame of cyber defense of values on which the organization is founded [13].

At the universal level, the matter of normative regulation of national cyberspace has so far only been superficially treated. Cyberspace is, namely, often presented as "open", "decentralized" and "participatory". Such view is not substantiated in international law. In the context of international security, UN Charter and international law apply in cyberspace and sovereignty and international principles, in regards to ICT and ICT infrastructure within state's territory [14].

Cyberspace can be perceived as a global domain in the framework of information medium of interconnected communication networks, [15] or as an interconnected network of IT infrastructures (the internet, telecommunication networks, computer systems and built-in processors and controllers), [16] including virtual surrounding of information and interactions between people. That is the space with parallel flow of processes of territorialization of cyberspace and cyber activities, as well as de territorialization, in the sense of deriving regulatory mandates from territories under the jurisdiction of organized societies [17]. An example is Internet Corporation for Asigned Names and Numbers (ICANN), which is however incorporated within the legal system of the US, through an agreement with the Department of Commerce, but has sole responsibility for maintaining the Internet safe, stable and interoperable. As cyberspace, with IoT era, becomes integral in every aspect of modern societies, it develops into a domain and medium through which are various human activities conducted [18]. Due to their inherent responsibilities, states are faced with an obligation to provide that national networks which support stability, prosperity and security of their citizens, remain effective and meaningful. The nature of the new challenges requires that the problem of decision-making legitimacy be addressed at international level [19].

An illustration of possible discrimination at the global level is provided by a couple of examples. One of such is a global cell phone game on public space, called „Pokemon Go“. An important consequence of this game, from the aspect of functioning of the society in omnipresent digital world, is privileged position of its owners, who use public space for making profits, without respecting national laws, concerning commercial fair activities, leasing of public land (since it is not making virtual, but real profit), nor taxation. The fact that this game is spreading on the global network, like the „smart“ appliances that are being produced without respect to national standards, cannot relieve a state of its responsibilities, when equality and safety of its citizens are concerned. Also, who can foresee the consequences of

the future development of one of the benchmark tasks of computer vision - scene recognition, and the effects it could have on individuals and their automatic recognition on the network. A state is financed to protect long-term interests and values of its citizens, and one of the prior concerns is general upholding national laws and nondiscrimination.

5. CONCLUSION

Massive production and emission of digital data broaden possibilities for their use for the benefit of private and public life. But, there are no objective indications which would found the assumption that limitless use of digital sources of data can result in "programmed" societal functions. That is the principle argument in favor of intrusive state approach to IoT in national cyberspace.

Apart from uncertain organizational effects, challenges of the IoT concept for organized societies include some specific threats concerning critical national infrastructure systems, guarantees for privacy, and ethical degradation as a consequence of adjustment to techno centric requirements.

Spreading of the IoT cannot be limited in administrative fashion, and from the aspect of the functioning of organised society, the solution is not in the practising of state authority to limit or censor the contents of networks.

But, on the other hand, it seems self-evident that no producer, provider, service or technology can have priority over the concerns for securing of social norms and standards, whether in city life, health care, or other fields of common interest in a society.

IoT additionally complexes the problem since it leads to unpredictably wider and more autonomous spectrum of communication and decision limitations. Living in an organized political society raises legitimate expectations that the apparatus that is paid by the citizens will not only protect basic value system founded on an individual but above define and regulate standards in common interest to which the implementation of IoT will have to adjust.

Governing and regulating (norming) societal impacts of the IoT, includes an in advance anticipation of at least the following issues: data protection and institutional changes to adapt to the IoT concept; responsibility for failures and breaches; status of devices that will obtain information about their users; applicable standards for business, industry, and public decision-making; and functioning of local and national policies within regional and global practices and policies.

REFERENCES

[1] Djurdjevic, Stevanovic, “The Value Challenge of Interconnectedness in Cyberspace for National Security,” in Sinteza 2016 - International Scientific Conference on ICT and E-Business Related Research, Belgrade, Singidunum University, Serbia, 2016, pp. 15-23; The Problem of Protecting Security of Persons and Property in Light of Development of IoT, Third ICT Security Conference, May 19-20, 2016, Belgrade.

[2] Freiman, Ori, “Towards the Epistemology of the Internet of Things: Techno-Epistemology and Ethical Considerations through the Prism of Trust”, International Review of Information Ethics, 22:12/2014, p. 6; McCraw, Benjamin, The Nature of Epistemic Trust, Social Epistemology, 29:4/2015, pp. 413-430.

[3] Haarkötter, Hektor; Weil, Felix, “Editorial”, International Review of Information Ethics, 22:12/2014, p. 1.

[4] Serrano, Martín et al., Executive Summary, in: “IoT Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps”, Serrano, Martín et al. (eds.), Brussels: European Research Cluster on the Internet of Things/European Commission, 2015, p. 6.

[5] Bibri, Simon Elias, “The Shaping of Ambient Intelligence and the Internet of Things: Historico-epistemic, Socio-cultural, Politico-institutional and Eco-environmental Dimensions”, Amsterdam: Atlantis Press, 2015, p. 39.

[6] Beltrame, Francesco; Dagostino, Virginia, “Advances in Internet of Things as Related to the e-government Domain for Citizens and Enterprises”, in: Advances onto the Internet of Things: How Ontologies Make the Internet of Things Meaningful, Gaglio, Salvatore; Lo Re, Giuseppe (ed.), Dordecht: Springer Science & Business Media, 2013, pp. 221-222.

[7] Neelie Kroes, “Creating tomorrow's Internet”, Speach at "Launch of Future Internet Labs", London, 3 September 2013, European Commission, p. 2.

[8] Talia, Domenico, “Towards Internet Intelligent Services Based on Cloud Computing and Multi-agents”, in: Advances onto the Internet of Things: How Ontologies Make the Internet of Things Meaningful, Gaglio, Salvatore; Lo Re, Giuseppe (ed.), Dordecht: Springer Science & Business Media, 2013, p. 276.

[9] Stevanovic, Djurdjevic, “The Capacity of Perception: The Need for an Educational System in Support of the National Security”, Creative Education for Employment Growth [The Fourth] International Conference Employment, Education and Enterpreneurship [EEE 2015], Belgrade, 2015, pp. 41-56.

[10] Ovidiu, Vermesan et al., “Building the Hyperconnected Society: Internet of Things Research and Innovation Value Chains”, Ecosystems and Market, Vermesan, Ovidiu; Friess, Peter (eds.), Aalborg: River Publishers, 2015, p. 80.

[11] A report of a workshop on the Internet of Things, “The Societal Impact of the Internet of Things” organized by BCS – The Chartered Institute for IT, on Thursday 14 February 2013. https://www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf, p. 4, 24.08.2016.

[12] Waher, Peter, “Learning Internet of Things”, Birmingham/Mumbai: Packt Publishing, 2015, p. 214.

[13] Ziolkowski, Katherina, “NATO and Cyber Defence”, in: Research Handbook on International Law and Cyberspace, Tsagourias, Nicholas; Buchan, Russell (eds.),

heltenham/Northampton: Edward Elgar Publishing, 2015, p. 427.

[14] UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN doc. A/68/98 (24 June 2013), paras 19-20.

[15] Kuehl, Daniel, "From Cyberspace to Syberpower: Defining the Problem", in: Cyberpower and National Security, Kramar, Franklin; Starr, Stuart; Wentz, Larry (eds.), National Defence University Press, 2009, p. 28.

[16] National Security Presidential Directive 54; also Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23).

[17] Brolmann, Catherine, "Deterritorializating International Law: Moving Away from the Divide between National and International Law", in: New Perspectives on the Divide between National and International Law, Nijman, Janne; Nollkaemper, Andre (eds.), Oxford: Oxford University Press, 2007, pp. 84-109.

[18] The White House, Cyberspace Policy Review: "Assuring a Trusted and Resilient Information and Communications Infrastructure", 2009. https://goo.gl/uUlxBx, 03.02.2016.

[19] Weber, Rolf; Weber, Romana, "Internet of Things: Legal Perspectives", Heidelberg: Springer, 2010, p. 86.