Government Cloud Computing and National Security

Hedaia-t-Allah Nabil Abd Al Ghaffar
Department of Political Science, Faculty of Economics and Political Science, Cairo University, Giza, Egypt

Received 19 September 2019
Revised 11 December 2019
Accepted 28 January 2020

Abstract

Purpose – The purpose of this paper is to try to reach the main factors that could put national security at risk as a result of government cloud computing programs.

Design/methodology/approach – The paper adopts the analytical approach to first lay foundations of the relation between national security, cybersecurity and cloud computing, then it moves to analyze the main vulnerabilities that could affect national security in cases of government cloud computing usage.

Findings – The paper reached several findings such as the relation between cybersecurity and national security as well as a group of factors that may affect national security when governments shift to cloud computing mainly pertaining to storing data over the internet, the involvement of a third party, the lack of clear regulatory frameworks inside and between countries.

Practical implications – Governments are continuously working on developing their digital capacities to meet citizens' demands. One of the most trending technologies adopted by governments is "cloud computing", because of the tremendous advantages that the technology provides; such as huge cost-cutting, huge storage and computing capabilities. However, shifting to cloud computing raises a lot of security concerns.

Originality/value – The value of the paper resides in the novelty of the topic, which is a new contribution to the theoretical literature on relations between new technologies and national security. It is empirically important as well to help governments stay safe while enjoying the advantages of cloud computing.

Keywords National security, Cybersecurity, Digital government, Government cloud computing, National threats, E-government

Paper type Research paper

Introduction

E-government studies have been recently focusing on new trends in the Information and Communication Technology (ICT) sector and how they relate to e-government development such as government cloud computing, Open Source programs, Artificial Intelligence, etc. Recent years have witnessed more government institutions worldwide moving to cloud computing in different state institutions and sectors, following the private sector's successful experience with cloud computing migration. Moreover, many countries drafted separate strategies to guarantee a more systematic and concrete migration to cloud computing such as the UK, Australia, Finland, France, Denmark, Austria, Germany, Ireland, Spain, Hong Kong, Japan, UAE, Palestine, Egypt, etc.

The shift to cloud computing is gaining momentum because of the great advantages expected out of the shift of institutions from traditional computing methods to cloud

Review of Economics and Political Science
Vol. 9 No. 2, 2024
pp. 116-133
Emerald Publishing Limited
e-ISSN: 2631-3561
p-ISSN: 2356-9980
DOI 10.1108/REPS-09-2019-0125

computing schemes. This is coupled with the increasing international economic crises and the increasing demands from the citizens, especially in the light of the international governmental attention paid to e-government development. Altogether, cloud computing provides a great solution to governments that introduces massive computing and storage capabilities at a reasonable cost compared to traditional computing and storage methods.

In addition, cloud computing is considered a massive transformation in the diverse processes of doing business such as data storage and processing as well as sharing data with others. However, as it is the case with every new technological transformation, cloud computing poses significant challenges and threats that come along with the tremendous advantages of the technology, especially concerns about information security and the required policies to ensure information safety (USA Department of Homeland Security – The President's National Security Telecommunications Advisory Committee, 2012, p. 1).

One of the major challenges that come along with cloud computing is the data security challenge. The study of data security within cloud computing environments is particularly important in the political science domain, based on the importance of data as a national strategic resource.

Data has always been a very important part of the national security concept, additionally, recent technological innovations have resulted in generating a massive amount of data worldwide, which is commonly known as "Big Data". Those data are analyzed and used by intelligence agencies worldwide in uncountable ways. Big data has easily replaced the work of millions of long-ago spies and agents (Van Puyvelde *et al.*, 2017).

Accordingly, studying the gaps where data breaches could happen has become an inevitable task, especially in the light of the fact that tens of governments worldwide are migrating their data storage and processing to the cloud, aiming at reaping the massive advantages of the cloud computing technology.

Advantages of cloud computing to governments

Cloud Computing refers to the abstraction of hardware, software, networks, storage spaces and services used by system developers to execute complex processes and to provide those facilities through the Internet. This kind of abstraction means that those hardware and services are "virtual" in nature; thus when using cloud computing, an institution does not have to buy new hardware or services, they just add new virtual storage spaces, for example, when in need and pay for them per use. Institutions can also stop using that virtual hardware or services when they no more need them and would then stop paying for usage. This is called a "pay-as-you-go" model, which has created a special competitive edge to the cloud computing technology. This is due to the fact that it empowers users to control and cut expenses tremendously through getting the job done perfectly and smoothly with the least expenses in comparison to investing in buying hardware, software and establishing massive data centers with all the affiliate costs of building, maintenance, cooling, updating, collocation (which is the process of creating another data center to hold back-ups) and others (Jamsa, 2013, p. 1, p. 3, pp. 45-49).

Some sources believe that the term "cloud computing" still lacks a clear definition, tending to regard cloud computing more of a wide concept that encompasses many technologies, rather than considering it a stand-alone technology (OECD, 2014, p. 8). One of the most common definitions of cloud computing is that of the NIST (USA National Institute of Standards and Technology), which states that:

> Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources e.g. networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction (NIST US Department of Commerce, 2013, p. 8).

Accordingly, cloud computing most competitive characteristics are (Ali *et al.*, 2015, p. 75):

- *On-demand self-service:* Customers can gain an increase in services or storage capacity over 24 h without the need to file requests or wait for approvals from the service provider. Cloud computing provides this luxury in a smooth, spontaneous and automatic way.
- *Broad network access*: Customers can access their data through the Internet via any device at any time from whatever place.
- *Resource pooling*: Cloud computing is built upon combining all resources (capacities, storage, data processing, etc.) in one place and putting them at the hands of different customers who share the usage of those resources collectively without the need to own and invest in them. Thus, achieving a tremendous cost-cutting advantage for customers and providers who enjoy the merits of economies of scale.
- *Rapid elasticity*: Customers can expand the requested services or shrink them easily and smoothly, or could even tailor cloud computing usage through a process called "cloud bursting" (Hill *et al.*, 2013, p. 29); which entails automatic shifting to the cloud once usage exceeds a specific limit. This could be of great benefit for banks, for example, which witness a significant increase in processing and demands during specific days of the month. Alternatively, those banks would have to invest in huge infrastructure, which would cover usage during peak days and would stay unused, (and therefore wasted opportunities) in other days.
- *Measured services*: Cloud computing usage can be controlled and measured. Therefore, customers pay according to the consumption "pay-as-you-go model".

The National Institute of Standards and Technology introduced classifications of cloud computing types, according to deployment models, (which describe the way resources are shared between customers) and service models, (which is a classification according to the services provided) (Jamsa, 2013, p. 3).

Cloud computing deployment models are classified as follows: public clouds (in which customers rent hardware and services via a service provider who owns data centers and resources and then sell them to customers who share resources collectively in a model called multi-tenancy and pay according to usage) (Hill *et al.*, 2013, p. 11), private clouds (owned by an institution where different departments share resources), community clouds (in which several institutions with a similar vision own and share data centers and resources) and hybrid clouds (combining features from more than one cloud type) (Hill *et al.*, 2013, pp. 23-31).

Typically, the above-mentioned cloud computing deployment models provide various security levels, ranging from more secured (private) to the least secured (public). They also provide different cost-savings models; ranging from the highest cost-saving model (public) to the least cost-saving model (private). This diversity renders the choices more complicated for governmental schemes of migrating to cloud computing (Hill *et al.*, 2013, pp. 5-6). Studies show that most governments that migrated to cloud computing resorted to the most secure and less cost-saving solutions, which is the private cloud. However, some governments, such as Australia, tend to classify data according to confidentiality and migrate data to different cloud types (Zwattendorfer and Tauber, 2013a, p. 6, p. 8).

Cloud computing service models classify the services provided to the customers as follows: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

Cloud computing technology seems a smart alternative to many governmental institutions around the world thanks to the numerous advantages that the technology provides, such as (Tweneboah-Koduah *et al.*, 2014, p. 3, p. 4):

- Clearly cutting governmental expenses through eliminating the need to invest in huge infrastructure capabilities especially all what is related to capital expenditure “CAPEX” and operational expenses “OPEX” (Jamsa, 2013); purchasing hardware and software, building data centers (and creating duplicate datacenters for backup, which is called collocation, maintenance of infrastructure, cooling facilities, hiring experienced IT personnel, etc.). Some studies estimated that governments can save up to 50-67 per cent of their expenses by moving to cloud computing (Zwattendorfer *et al.*, 2013b, p. 184).
- Easy scalability; which is a unique characteristic of the cloud computing technology, where an institution can cope with the increase or decrease in workloads without any additional costs, thanks to the possibility of adding hardware and software when in peak times and then removing additional resources when off-peak. This is possible because of the core idea of cloud computing, which is “virtuality” of hardware and software that makes adding and removing resources an easy process.
- Increased productivity; as cloud computing provides a smart mechanism for governments to implement their digital government strategies and to meet citizens increasing needs effectively and efficiently. This is possible thanks to cloud computing that enables accessing governmental services anywhere over 24 h, eliminating bureaucratic complications and corruption, and therefore, achieving good governance standards.

Cloud computing and national security relate to each other through “cybersecurity”

Despite the great advantages that cloud computing provides, there are some drawbacks to the technology that might expose data privacy and confidentiality to dangers. These dangers stem from the fact that cloud computing facilities are provided through the internet and maybe through a service provider that may reside in another country, where different laws for data protection might be in action.

In case of governments using cloud computing, concerns about data protection and national security arise. However, we need to carefully tackle the topic to avoid reaching conclusions about unrelated concepts; can government cloud computing affect national security? How do the concepts relate?

As a start, we should study what the concept of “national security” means. Despite the great importance of the national security concept, it is a matter of fact that efforts to define the concept are relatively poor and that academia for some unknown reasons disregarded defining the concept. Literature about national security has focused otherwise on normative arguments concerning determining the core values that should be included and protected under the umbrella of national security, defining political agendas in terms of national security, arguments about the nature of national security threats, etc. According to some scholars, these factors, among others, have resulted in poor literature on defining national security. This belief is based on a comparison between academic contributions about defining national security concepts versus other political concepts such as power, justice and freedom (Baldwin, 1997, p. 5, p. 9).

Barry Buzan described the national security concept as an "underdeveloped concept", as opposed to what the norm is in defining concepts in Political Science. Buzan stated that despite using the concept on a wide scale politically, and despite being a core concept in countries policies, literature had only been concerned with the application of the concept (such as what values should be protected, what is the level of protection, what are the levels of security; whether individual or society or state, etc.) rather than focusing on establishing a strong conceptual base.

Buzan presented some possible explanations to this academic disregardment to defining the term "national security"; he proposed some reasons related to the difficulty of the term and its overlapping with some other terms such as power. Another possible explanation presented by Barry Buzan relates to the appeal of this ignorance to policymakers so that they would have the opportunity for relative and loose interpretations of the term "national security". However, Buzan finally believed none of these reasons are valid in anyways.

According to Barry Buzan, national security is "freedom from threat and ability of states to maintain independent identity and their functional integrity against forces of change, which they see as hostile" (Buzan, 1991, p. 432).

Arnold Wolfers, on the other hand, emphasized the fact that the concept of "security" is an "ambiguous symbol" (Baldwin, 1997, p. 6) and that security as a political value is very much related to the individual and society value systems. Wolfers believed that the definition of the term "security" is the double-sided; objective and subjective dimension of security. Objectively, security means "the absence of threats to acquired values" and subjectively, security is "the absence of *fear* of threats to acquired values." (Wolfers, 1952, p. 484, p. 485).

Security is achieved, from an objective side, when it is possible to overcome threats, challenges and vulnerabilities and to handle them on the individual and society levels. Despite the importance of the objective factors in defining security, subjective factors have a considerable impact on the definition of security, especially in the light of the fact that realizing and defining threats depends on the personal and subjective views of policymakers, which, in turn, depend on personal and cognitive views and references. This results in great differences between policymakers' views about threats, challenges and vulnerabilities, which finally creates a variable concept of "security" between policymakers, individuals and societies, as well as variable security-related concepts such as threats, challenges and vulnerabilities (Buzan, 1983, p. 73).

The national security concept has undergone several changes over the years, especially in the wake of the end of the Cold War and the rise of globalization, which had its impacts on all life aspects. Globalization and ICT developments had their impacts on national security as well; as threats turned to be much more abstract and complex.

The nature of the relationship between concepts of information security, cybersecurity and national security has been a matter of scholar debate for years. As a matter of start, there is some kind of overlap and confusion between the terms "information security" and "cybersecurity", which needs clarification first. Information security refers to:

> [. . .] everything about protecting the information, which generally focuses on the confidentiality, integrity and availability (CIA) of the information. On the other hand, cybersecurity is about securing things that are vulnerable through ICT. It also considers where data is stored and technologies used to secure data. Part of cybersecurity is about the protection of information and communications technologies – i.e. hardware and software (Cisco Platform, 2016).

According to the National Institute of Standard and Technology, cybersecurity is "the ability to protect or defend the use of cyberspace from cyber-attacks." Information security refers to "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction to provide confidentiality, integrity and availability" (Paulsen and Byers, 2019, p. 58, p. 94).

Accordingly, it can be concluded that cyber security is much more inclusive than information security. It is also worth mentioning that information security is not a new concept, it is older than the cyber security term[1].

Since the coinage of the cyber security term, it has been controversial whether or not to include cyber security as a part of national security domains; whether it should be studied as a field of security studies instead of studying cyber security within technical or legal frameworks (Hare, 2010, p. 213).

Some literature stated that there is a kind of exaggeration in linking cyber security with national security. Their argument is mainly based on the belief that cyber attacks usually target networks and systems rather than infrastructure. Consequently, it is expected that the damage caused by cyber attacks would be less than that caused by military attacks that usually target states infrastructures and threaten citizens' security.

Additionally, it is argued that destroying infrastructures or targeting huge damages are not feasible through one cyber-attack; several cyber-attacks are needed to achieve considerable damage. In fact, this is hard to be done because information security systems are designed to discover attacks on the spot and deal effectively and timely in response to cover up vulnerabilities. Launching another cyber attack would take time to discover new vulnerabilities to attack.

Consequently, some writings believe that cyber security should not be a part of national security; because the damage caused by cyber-attacks is a normal damage that only cause financial loss and that it is not the type of threats that cause damages to infrastructure and would, in this case, need exceptional measures to face it. "Cyber attacks, unless accompanied by a simultaneous physical attack that achieves physical damage, are short lived and ineffective" (Lewis, 2002, p. 3, p. 11).

Other scholars believe that cyber attacks can only be a threat to national security when infrastructure is a vulnerability, when daily activities are highly dependent on remote computer networks and when governments tend to save data over the internet, which is the case of nowadays governments shifting to cloud computing. At that time, governments should balance those risks through powerful security systems and strong active legal frameworks as well as taking whatever needed measures to secure national infrastructures (Lewis, 2002, p. 11).

Different views about the relation between cyber security and national security strongly relate to views about the scope of national security definition. Neorealists believe cyber security should not be a part of national security, this is based on their views about national security scope of the definition. Neorealists believe national security is related to military threats and everything, that is, related to military wars. Cyber attacks, in their views, still have not proved to affect the tangible security of countries and national infrastructures.

Stephen Walt is one of the prominent figures of this state-centric traditionalist trend in defining security. Walt restricts security threats to those of a militant nature only, and he equates security with the absence of military conflicts. Walt defines security as:

> [. . .] the study of the threat, use and control of military force. It explores the conditions that make the use of force more likely, the ways that the use of force affects individuals, states and societies, and the specific policies that states adopt in order to prepare for, prevent, or engage in war (Tarry, 1999, p. 2).

The traditionalist scope of security was undoubtfully criticized based on many grounds, such as the failure to capture other security threats in the modern real world, especially those that encompass soft power threats to national security, such as cyber threats.

On the other hand, other scholars adopt a wide view about the scope of national security threats such as military, political, economic, social and environmental threats, etc. They believe that national security threats should not essentially target national infrastructures. According to this group, national security threats should include everything that threatens individuals, institutions, companies, societies or countries (Hare, 2010, p. 214). The Danish Peace Research Institute and Copenhagen School for security studies, which contributed a lot to security studies and which Barry Buzan belongs to, adopts this wide view of security.

Mohammed Ayoob, one of the pro "wideners" trend in defining security, views that "national security is a function of state-building, which requires that a state possesses more than simply not only "security hardware" (control of coercive force) but also "security software" (legitimacy and integration)." Ayoob defines security as:

> Security or insecurity is defined in relation to vulnerabilities, both internal and external, that threaten to, or have the potential to, bring down or significantly weaken state structures, both territorial and institutional, and regimes (Tarry, 1999, p. 3).

Michael Klare and Daniel Thomas also believed that the concept of security needs to be expanded because of a "declining significance of geographical boundaries". Instead of focusing on domestic threats, they adopted a global view of security. According to Klare and Thomas, security is: "security involves more than protection against military attack [. . .] ecological, economic and demographic trends pose serious challenges to developed countries" (Tarry, 1999, p. 6).

The problem with widening the scope of national security threats to more than the military is that the criteria of defining threats become very subjective in nature. In an effort to introduce reasonable criteria, Buzan defined national security threats as: "security is about survival; it is when an issue, presented as posing an existential threat to a designated referent object, justifies the use of extraordinary measures to handle them" (Šulovic, 2010, p. 3). This has, in turn, led to the introduction of what Buzan called "securitization process"; which means transferring different topics that are supposed to be a possible threat to national security from its normal framework to what is called "panic politics" or panic agendas.

Another trend in defining security, known as the "deepening trend", focuses on determining the referent object itself rather than studying factors that should be included in the security definition. This trend allows for a more comprehensive view of the referent object to include individuals and societies rather than focusing on the state as the main referent object (Tarry, 1999).

Aside from the theoretical debate about posing cyber security in the domain of national security, some believe that it is more useful to study how countries are dealing with the topic empirically and whether countries consider cyber threats as potential national security threats or not.

The USA comes on top of countries that consider cyber threats as potential national security threats and this was evident in several speeches and statements, especially since 2009 (during Obama's rule) (Chauvin, 2016). Barack Obama referred during his speech in 2009 that his administration is very much concerned with cybersecurity as a part of the USA political, military and economic policies, where he stated that: "it is now clear that cyber threat is one of the most serious economic and national security challenges we face as a nation" (The White House, 2009).

Barack Obama asserted that digital infrastructures in the USA are treated as “national strategic assets”, and therefore should be protected, and has consequently launched the Comprehensive National Cybersecurity Initiative and a special unit for cyber security was established inside the USA Department of Defense (DoD), called “USCYBERCOM”. The USA DoD went beyond this to declare that cyber space is officially considered the “fifth domain of military intervention, just as critical as land, sea, air and space” (Lynn, 2010, p. 101).

The USA administration believes that cyber threats could lead to physical destruction equivalent to that of mass destruction. A responsible in the Department of Defense described cyber threats as “cyber Pearl Harbour” and that it “could cause physical destruction and loss of life” and “be as destructive as the terrorist attack 9/11” (Bumiller and Shanker, 2012).

These speeches and policies prove with no doubt that the USA considers cyber threats as real potential threats to the country’s national security. Many other countries, of course, react in the same way by considering cyber threats potential national security threats to their countries.

National security concerns pertaining to government cloud computing

First: Threats related to the nature of cloud computing

- *Multi-tenancy security problems*: Cloud computing is based on renting infrastructure to other users so that there are several customers sharing the same infrastructure. If technical problems took place, through cyberattacks on what is called the Virtual Machine Monitor or the hypervisor, which is responsible about separating virtual machines, customers’ data may be exposed to each other (Hashizume *et al.*, 2013).

Additionally, data that have been deleted before may be retrieved by another malicious customer, which exposes data privacy to dangers. Cloud providers sometimes resort to what is called the “data wiping” technique; so that when a customer no longer wants the data he/she not only deletes the data but also rewrites symbols and numbers over what was written before to completely wipe the data and keep no track of it:

- *Vendor lock-in*: Some cloud service providers sell unpopular or tailored programs and services, which creates a problem for the customers in case they no longer want to keep their data with the service provider. *Customers* may encounter technical problems related to transferring data to another service provider; so customers would be “locked-in” with a given service provider and forced to keep their data with this specific provider despite that he may have violated the contract or provided unsatisfactory results. Some service providers overcome this problem by using open-source programs and software.
- *Failure of service provider*: To protect customers from the possibility of service providers failure, which would, in turn, expose customers data to threats, some companies provide a “source code” of customers data and software to a third party. Customers can then easily switch to the third party in case of the failure of the original cloud service provider. However, this would involve rearranging legal matters with the third party (Hill *et al.*, 2013, p. 129, p. 131).
- *Expanding the network of employees who are authorized to view data*: One of the security threats related to cloud computing is the anonymity of the IT personnel responsible for the customers’ data in the data centers. Normally, governmental institutions invest in their IT personnel who are authorized to view data, but, that is,

not the case in cloud computing (Hashizume *et al.*, 2013, p. 6). Despite the fact that governments usually migrate insensitive data to the cloud, institutions should pay attention to other new technologies, such as "Big data analytics" that depend on analyzing small insensitive data and reaching accurate conclusions about individuals, institutions and nations, in a process called "mass profiling".

- *Interdependency and difficulty of specifying the responsible for security breaches*: The cloud computing environment is characterized by distributing tasks and responsibilities to achieve a considerable decrease in costs. Despite the fact that this kind of "interdependency" helps in reducing costs and workloads, it causes, on the other hand, an interdependency in security and loss of track of the responsible entity or person (Iqbal *et al.*, 2010, p. 6, p. 7).

This is in addition to another kind of dependency between deployment models (SaaS, PaaS, IaaS); as software and platforms are hosted on infrastructures. If we add to this the fact that sometimes each service is provided by a separate service provider, one can imagine how far security dependency is a real concern and can lead to a loss of track of who is responsible about security breaches.

In this regard, it is worth mentioning that using Infrastructure as Service is the most secure choice because the customer determines in this case how to host software and platform on the infrastructure and would consider security concerns.

Based on the above, cloud computing literature gives special attention to "Cloud Governance", which implies assigning the task of observing all the processes and components of the cloud environment to a specialized entity to ensure security in the cloud environment:

- *Data security*: One of the cloud computing basics is creating back-ups of all data stored in a data center in another duplicate data center far away from the original one, a process called "colocation". This idea is a major security concern; especially that data can move between data centers around the world, so in case of security breaches, there would be complications about when did the breach happen, in what country and under what jurisdiction. The fact that cloud computing regulations are still immature or absent in many countries just complicates the scene (Hashizume *et al.*, 2013, p. 4, p. 5).

Encrypting data is one of the most popular solutions to securing data while transferring it, however, it should be noted that some countries laws prevent encrypting data, in addition to that encryption cannot technically apply to all deployment models; data can be encrypted on IaaS but it cannot be encrypted on SaaS and PaaS (Backe and Lindén, 2015, p. 15).

Blockchain-based solutions are also a popular way to secure data in the cloud environments. It has originally been introduced with the Bitcoin cryptocurrency, however, gained momentum of usage afterward in other areas because of the security advantages in provides. The blockchain technology is:

> [. . .] a structured list that saves data in a form similar to a distributed database and is designed to make arbitrarily manipulating it difficult since the network participants save and verify the blockchain (Park and Park, 2017, p. 2).

Studies found that if blockchain solutions were introduced to the cloud computing environment it would bring about higher security probabilities, because of the decentralized security nature of the blockchain technology.

Technical threats

A considerable portion of cloud computing literature provided a number of technical threats and attacks and provided technical solutions to them as well. As the topic of this article is political in nature, the technical threats would be better studied by specialists. Some technical threats that could lead to security problems are: distributed denial of service attacks (DDoS), packet sniffing attacks, guest-hopping attacks, etc.

Legal threats. Legal threats pertaining to cloud computing arise from the fact that cloud computing service provider is subject to different legal and judicial jurisdictions of different countries at the same time; such as the user's country, the country where the service provider is located and countries where the data passes through. Things get more complicated in cases of contradiction between laws and regulations of different countries regarding rights, data protection, data encryption, data destruction, data disclosure to state authorities, etc. (Iqbal *et al.*, 2010, p. 8).

In the light of the absence of cloud computing regulations in many countries and in the light of the transnational impact of this absence of regulations, international organizations give due care to cloud computing legislations. This special attention is based on the belief that the increase of electronic crime rates coupled with complication of cloud computing jurisdiction specification, expose the rule of law to danger; as countries stand powerless against completing their investigations in different cases because of the different legislative obstacles and other countries sovereignties (Council of Europe – Cybercrime Convention Committee T-CY, 2016, p. 7).

The past few years have witnessed several incidents of communications and data disclosure related to individuals, even if that transcends country's borders, especially in the absence of international regulations of cloud computing (De Hert and Boulet, 2013, pp. 23-26). Several examples could be cited in this regard; the Belgian Supreme Court, for example, held that the legal articles related to crimes in Belgium "Belgian Code of Criminal Procedures" can apply to a foreign electronic service provider to disclose information required: "Article 46bis of the Belgian Code of Criminal Procedure (CCP) can also be applied to a foreign provider of electronic communications services (Yahoo!) to hand over identification data" (De Hert and Boulet, 2013, pp. 23-26).

Additionally, the Belgian lawmaker allowed investigation authorities and judges in Belgium to extend their search and investigations on all systems and networks inside Belgium and outside it without the need to a formal request and without requests of mutual cooperation between countries. This should only take place in cases of necessity and the fear of loss of evidence in cases of critical crimes and should be accompanied with a posteriori notification:

> [. . .] the Belgian lawmaker created the power of the network search (Article 88ter CCP) allowing an investigative judge, when performing a search on a computer system, to extend this search to another computer system even outside the Belgian borders and without formal request for mutual legal assistance. The extraterritorial reach of this network search has been justified by considerations of time and risk of evidence loss in cases of serious crime, but backed by principles of necessity, proportionality and a posteriori notification (De Hert and Boulet, 2013, p. 24).

It is generally believed that in the absence of international legal frameworks for cloud computing, countries can protect their cyber security in whatever way. Additionally, the European Council Cybercrime Convention Committee praised the Belgian solution, emphasizing that those practices provide good solutions for data stored in the clouds:

> [. . .] the Belgian solution offers great opportunities to handle data stored in “the cloud”. [. . .] [and] makes clear that it is not important to know where the data is stored, but from where it is accessible. (Council of Europe - Cybercrime Convention Committee T-CY, 2012, p. 33).

On another hand, the Tallinn Manual on the International Law Applicable to Cyber Warfare, prepared by international experts and presented in the NATO Cooperative Cyber Defense Excellence, provided that states can exercise their jurisdiction of extraterritorial reach in line with international law (Council of Europe – Cybercrime Convention Committee T-CY, 2012, p. 24). The Manual recognizes the impact of cloud computing on changing nature of states jurisdictions: “state shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other states” (Schmitt, 2013, p. 33).

In light of these worldwide actions and the international approval of extraterritorial reach jurisdictions of countries, private companies have been trying to assure their customers about the safety of their data and to prove themselves irresponsible for any acts of data disclosure. Microsoft and Google have been publishing transparency reports about their cooperation with Law Enforcement Agencies (LEAs) (De Hert and Boulet, 2013, p. 25).

Accordingly, specific legal threats of government cloud computing can be summarized as follows (Council of Europe – Cybercrime Convention Committee T-CY, 2016, p. 7, p. 8, p. 9):

(1) Location:

- It is usually unclear under which state’s legal jurisdictions shall the data be treated; because the main location of the service provider may be in country A, while data centers may reside in country B and duplicate data centers may be in country C and D or more. Things get more complicated because these data and duplicates usually transfer easily between countries without prior notification to the data owner as those activities are considered normal in the light of load-balancing between data centers or for preventing criminal access.
- Even in case of holding data in the same location and in case of identifying this place, it is still legally controversial, which laws to apply in cases of security breaches or unlawful access and usage of data stored in the clouds. Some believe that the main criteria for identifying jurisdictional responsibility shall be the main headquarter of the service provider (taking into considerations that there may be more than one main headquarter and maybe affiliates to main headquarters). Others believe it shall be the location of data. Others believe it shall be the country where the unlawful action took place. Others believe it should be the country that the suspect holds its nationality. Countries develop data protection laws to try to handle these kind of issues. However, not all countries have data protection laws and not all countries' laws are detailed in these regards.
- It is still unclear whether the data controller is the same as the data processor.
- Some considerations may arise regarding the anonymity of the original owner of data and the data stored via transnational co-hosting solutions.

(2) The cloud service provider is subject to different legal jurisdictions at the same time:

- Pertaining to data protection: Data protection jurisdictions in European Union (EU) countries, for example, is based on the location of the data controller, even if the processing took place outside the EU countries.

- Pertaining to taxes: Legal jurisdictions in the EU, for example, is determined not by the location of the international headquarter, servers or data controllers, but based on several other considerations, such as the location of the subsidiary doing businesses.
- Pertaining to consumer protection: According to the general data protection regulation (GDPR) of the EU, it is usually based on the consumer's location.
- Pertaining to intellectual property rights: In civil cases, jurisdiction is based on the location of the business, while in criminal cases, jurisdiction is determined according to the location of the perpetrator.

(3) As mentioned earlier, cloud computing allows combining more than one deployment model; software, platform and infrastructure service providers may collaborate together and share doing the same task, which creates security dependency and an overlap of legal responsibilities.

(4) Governments can issue interceptions to electronic service providers to disclose information: electronic service providers are obliged to disclose customers' data in case of being asked by courts and authorities to disclose clients' data for tracking suspects. These cases are very complicated because they include overlapping of jurisdictions between countries and a lot of legal issues as a result of the transnational nature of cloud computing.

(5) Other concerns raised by cloud computing are related to how to ensure that data controllers and processors are obliged to notify customers with data breaches, and the unclear nature of cloud computing companies in some countries and the legal jurisdictions they are subject to.

Countries' reactions toward national security concerns related to cloud computing

As clarified in the previous section, challenges pertaining to cloud computing are both legal and technical, and consequently, many countries introduced several laws and regulations in different areas to try to cover technical and legal challenges. Not to mention, trying to overcome legal security challenges alone would have the country to introduce several laws or amendments to laws and regulations. For the purpose of a political science study, the paper will try to shed light on the main trends regarding legal actions introduced by countries to overcome only the challenges of data security stored in the clouds.

Snowden revelations that were disclosed several years ago have shown a kind of unclear relation between giant US tech companies and the US national security agencies, as well as the UK government that has been involved in the Snowden data revelations scandal through different security programs, the most famous of which are PRISM, TEMPORA and MUSCULAR. The Snowden data infringement revelations uncovered the fact that US tech companies are obliged to disclose customers' data stored in data centers located on the American land. This is usually done through the issuance of a legal permission from an American court (Hill, 2014, p. 5).

Those incidents raised several concerns about data privacy in the clouds, especially when it comes to dealing with American giant tech companies. This is particularly important in the light of the lack of a unified data protection regulation in the USA, which renders legal matters either regulated by industry-specific regulations or special states regulations or other countries' regulations. Accordingly, in some cases, legal issues may take place within an ambiguous jurisdictional reference.

Several reactions were cited regarding protecting data in the clouds from countries, and from the US companies who tried hard to prove themselves capable of protecting customers' data in the clouds through several ways. In this regard, it is worth mentioning that Microsoft sued the USA. security apparatus for trying to oblige it to disclose e-mail records in Ireland, while The International Business Machines Corporation started investing billions of dollars for constructing several data centers outside the American territory in the aftermath of the Snowden revelations (Hill, 2014, p. 8).

Countries reactions have varied greatly, but it can be said that some of the prominent reactions had been: first the European response with the release of the GDPR and replacing the safe harbor agreement with the EU–USA Privacy Shield regarding the relation with the USA, second the introduction of data localization laws in several countries such as Russia, China and some other Asian countries.

In the wake of the American data revelations scandal that uncovered data privacy breaching acts conducted by the USA, several European suggestions went for proposing and implementing data localization solutions (such as France and Germany), emphasizing the necessity of passing laws and regulations that would guarantee data and infrastructure localization. Data and infrastructure localization refers to passing laws and regulations that would limit data storage and data movement and processing to specific geographical areas or determining companies allowed to manage data according to the company's location and its nationality (Hill, 2014, p. 3).

After years of studying proposals and negotiations, the European Union came out with the GDPR, that is, binding to all European countries, and which actually became a model law for many countries in different continents. The GDPR took effect on the 25th of May 2018, replacing the old EU Data Protection Directive, which was the main reference in regulating data protection in the European Union since 1995. It is worth mentioning that the GDPR regulates personal data in the EU, while the non-personal data is regulated by the Regulation on the Free Flow of Non-Personal Data, which took effect on the 28th of May 2019. Both laws are applied for data protection in the European Union within the EU Digital Single Market Strategy.

The GDPR became a model law for many countries because of the expansion of users' rights within the law and the widened scope of data protection provided through its provisions. Some of those rights granted in the law are as follows: (Official Journal of the European Union, 2019):

- *Increased territorial scope*: GDPR applies to all companies that hold and process personal information pertaining to individuals residing in the EU, regardless of the location of those companies. A data officer to the EU is supposed to be appointed by companies holding European resident's data.
- *Penalties*: One of the main changes introduced by the GDPR are the penalties applied to the companies breaching the GDPR, which can reach 4 per cent of the annual revenue of the company or $20m (the greater applies).
- *Consent*: GDPR has regulated gaining consents from users so as not to be long, vague and unreadable. Consents should be provided in an easy straightforward way and the aim of data collection should be stated inside the consent. Additionally, withdrawing consents should be as easy and clear as providing consents.
- *Breach notification*: Breach notification should be provided without undue delay, and should be done within 72 h of discovering data breaching.

- *Right to access*: Users have the right to get a confirmation from data controllers and processors whether their data is being held and processed or not. They can gain information about the aim of holding their data and the place where the data is stored.
- *Right to be forgotten*: This is also known as "right of data erasure", where users have the right to get the data controller to erase their personal data and stop collecting more data whenever they want.

On another hand, the EU had their data protection affairs with the USA regulated over several years ago through the Safe Harbor Agreement. Based on the difference between the strict EU data protection system versus the loose American data protection system, the Safe Harbor Agreement was designed to regulate EU data protection matters when transferred and stored in the USA (Privacy Shield Website) The Safe Harbor Agreement depended on validating American companies each on its own from the side of the EU to assess whether it is safe to transfer the European data to them or not, and it has been in effect since 2000 (Chabinsky and Pittman, 2019). However, the Snowden revelations and the Max Schrems ruling (an Austrian activist who sued Facebook for disclosing European data to the US security apparatus) have proved the Safe Harbor failure, so it was canceled in October 2015 according to the EU Court of Justice ruling.

The Safe Harbor Agreement was replaced by the EU-US Privacy Shield Law on the 12th of July 2016, which aimed at providing more protection for the European data whenever transferred or stored in the EU. The difference between the Safe Harbor and the EU-US Privacy Shield lies mainly in the mechanisms of data transfer and the related rights, providing remedies to the extensive USA reach to the EU citizens data and the weak rights provided to the users against the American data processors and controllers (Terpan, 2018).

Main protection tools introduced by the EU-USA Privacy Shield can be summarized as follows: (Otava, 2019)

- *Increased European individual rights*: European individuals are given the right to sue American companies for data breaching through several ways, one of which is the Privacy Shield Panel, specialized in reviewing such cases.
- *More strict requirements for American companies to be accredited to work with EU data*: Requirements for accrediting USA companies to work with European data had turned much stricter. Companies are accredited on an annual basis from the side of a special European entity, according to abiding by the law's provisions.
- Restricting the American security apparatus reach to European data; where the USA Department of Justice and the CIA both signed on provisions limiting their reach to European data. Those guarantees are also reviewed on an annual basis.
- *Third parties are equally liable*: Third parties are totally responsible about data protection and should pass by the same accrediting process as the original party.

Another trend of data protection is the data localization laws and requirements applied by countries to secure data protection. Different countries applied different levels of data localization and in different areas, some are explicit (*de jure*) and others are implicit (*de facto*). Some countries such as Russia, China and Iran, applied data localization on a wide scale, requiring saving citizens' data on internal servers located on the territories of the country. Other countries have applied partial data localization, such as Canada that puts restrictions on governmental entities so that data are being saved in Canada (Chander and

Le, 2014, p. 7). Other countries resorted to requiring governmental institutions to purchase ICT and storage equipments locally, while others imposed restrictions on employment in data centers, requiring hiring local workforce in data centers.

It is worth mentioning that data localization is being criticized by many on the grounds that it is considered a backstep in the developmental path of the internet and information society, as it may have a negative impact on the global economy due to restricting the free flow of information on the internet. On another hand, opponents to data localization requirements argue that those laws originally target securing data from censorship, while end up with governments practicing censorship on their citizens freely, as a result of the centralization of citizens' data inside the country (Hill, 2014, p. 3).

In fact, as it is clear now, it is a very complicated task to try to achieve a high level of data security while enjoying the merits of cloud computing. No matter what strategy chosen by countries to achieve data security goals, it should be carefully studied, especially in the light of many other variables, to mention a few, namely, the local, regional and international regulatory ecosystem, the country's political, social and economic cultures and statuses, the country's technological maturity level, [. . .], etc. Each country has its own particularity in regards to cultures, economic and political structures, historical background, etc. Those particularities impact in a way or another the decisions of countries and their choices of strategies. For example, we saw Germany and Brazil, in the aftermath of the Snowden disclosures, proposing solutions favoring data localization solutions, such as the Online Privacy Resolution presented collaboratively to the UN suggesting establishing fiber-optic cables between Europe and South America without the need to pass by the USA. Some studies found a common ground historical reasoning for such proposals based on the past sufferance from citizen censorship carried out by dictatorship systems in both countries (Chander and Le, 2014, p. 7).

Conclusion

Government cloud computing is a very hot topic on both national and international agendas. Governments are very much keen on incorporating this new technology in their e-government programs to benefit from the advantages that the technology provides. However, it is of no doubt that there are some security concerns attributed to the technology that could have considerable effects on data security. International organizations are currently working on studying national and international regulations related to cloud computing and data security in order to provide international legal frameworks for cloud computing. Each country planning to migrate to cloud computing should study first what are all the possible implications of government cloud adoption on all levels. Governments should particularly study their national laws and regulations related to cloud computing as well as other countries' rules and regulations because cloud computing creates a very complicated interconnected environment. Countries implement different strategies to ensure the highest possible security level, however, each strategy has its own pros and cons. Each country should also assess what serves its goals and fits with its own regulatory, social, political and economic particularities. Most importantly, cloud computing security strategies' success should be assessed regularly and accordingly updated and modified.

Note

1. For more detailed definitions of information security and cyber security and related definitions, please check "compilation of existing cyber security and information security related definitions" report.

References

Ali, O., Soar, J. and Yong, J. (2015), "An investigation of the main factors to be considered in cloud computing adoption in Australian regional local councils", *Journal of Contemporary Issues in Business and Government*, Vol. 21 No. 1, pp. 75-93, available at: www.researchgate.net/profile/Omar_Ali22/publication/289398040_An_Investigation_of_the_Main_Factors_to_be_Considered_in_Cloud_Computing_Adoption_in_Australian_Regional_Local_Councils/links/56df9d7408aec4b3333b791f/An-Investigation-of-the-Main-Factors-to-be-Considered-in-Cloud-Computing-Adoption-in-Australian-Regional-Local-Councils.pdf (accessed 7 July 2019).

Backe, A. and Lindén, H. (2015), *Cloud Computing Security: A Systematic Literature Review, Degree Project*, Uppsala University, Uppsala, available at: www.divaportal.org/smash/get/diva2:825307/FULLTEXT01.pdf (accessed 20 September 2018).

Baldwin, D. (1997), "The concept of security", *Review of International Studies*, Vol. 23, pp. 5-26, available at: www. princeton.edu/~dbaldwin/selected%20articles/Baldwin%20(1997)%20The%20Concept%20of%20Security.pdf (accessed 17 August 2018).

Bumiller, E. and Shanker, T. (2012), "Panetta warns of dire threat of cyberattack on U.S", The New York Times, October 11, available at: www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html (accessed 20 September 2018).

Buzan, B. (1983), *People, States and Fear: The National Security Problem in International Relations*, Wheatsheaf Books, Hemel.

Buzan, B. (1991), "New patterns of global security in the twenty-first century", *International Affairs*, Vol. 67 No. 3, pp. 431-451, available at: http://home. sogang.ac.kr/sites/jaechun/courses/Lists/b7/Attachments/10/New%20Patterns%20of%20Global%20Security%20in%20the%20TwentyFirst%20Century_Buzan.pdf (accessed 12 January 2019).

Chabinsky, S. and Pittman, F.P. (2019), "USA: data protection 2019", available at: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Chander, A. and Le, U.P. (2014), "Breaking the web: data localization vs the global internet", UC Davis Legal Studies Research Paper Series, (378), available at: http://ssrn.com/abstract=2407858 (accessed 28 November 2019).

Chauvin, J. (2016), "Book review: cyber war will not take place", *Interstate – Journal of International Affairs*, Vol. 2015/2016, No. 2, p. 1, available at: www.inquiriesjournal.com/articles/1342/book-review-cyber-war-will-not-take-place (accessed 20 April 2019).

Cisco Platform (2016), "Understanding difference between cyber security and information security", available at: www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information (accessed 17 May 2019).

Council of Europe – Cybercrime Convention Committee T-CY (2012), "Discussion paper: transborder access and jurisdiction: What are the options? Report of the Transborder Group", Adopted by the T-CY, Strasbourg, 6 December, available at: www.coe.int/t/dghl/standardsetting/tcy/TCY2012/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf (accessed 24 November 2018).

Council of Europe - Cybercrime Convention Committee T-CY (2016), "Criminal Justice Access To Electronic Evidence In The Cloud: Recommendations For Consideration By The T-CY Final Report Of The T-CY Cloud Evidence Group", Strasbourg, 16th of September, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e (accessed 24 November 2018).

De Hert, P. and Boulet, G. (2013), "Cloud computing and trans-border law enforcement access to private sector data", *Challenges to Sovereignty, Privacy and Data Protection' in Workshop Paper Collection 'Big Data and Privacy: Making Ends Meet*', 10th of September, CA Stanford Law School: Future of Privacy Forum and the Centre for Internet and Society, pp. 23-26, available at: https://fpf.org/wp-content/uploads/Big-Data-and-Privacy-Paper-Collection.pdf (accessed 13 March 2019).

Hare, F. (2010), "The cyber threat to national security: Why can't We agree?", in Czosseck, C. and Podins, K. (Eds), *Conference on Cyber Conflict Proceedings*, CCD COE Publications, Tallinn, Estonia, pp. 211-225, available at: www.cpahq.org/CPAHQ/CMDownload.aspx?ContentKey=e1bcfabc-c472-4b35-9d89-f7108fc2f597&ContentItemKey=c9308b04-a4f2-4d36-9889-010dbfd03c78 (accessed 28 May 2019).

Hashizume, K., Rosado, D., Fernández-Medina, E. and Fernandez, E. (2013), "An analysis of security issues for cloud computing", *Journal of Internet Services and Applications*, Vol. 4 No. 1, pp. 1-13, available at: www. jisajournal.com/content/4/1/5 (accessed 29 July 2019).

Hill, J. (2014), "The growth of data localization post-Snowden: analysis and recommendations for US policymakers and industry leaders", *Lawfare Research Paper Series*, Vol. 2 No. 3, pp. 1-34, available at: papers.ssrn.com/sol3/papers.cfm?abstract_id=2430275 (accessed 17 November 2019).

Hill, R., Hirsch, L., Lake, P. and Moshiri, S. (2013), *Guide to Cloud: Principles and Practice*, Springer, London, doi: 10.1007/978-1-4471-4603-2.

Iqbal, A., Black, B., Fisher, C., Cella, J., Abrams, J., Dugi, M. and Leventhal, R. (2010), "Cloud computing and national security law", The Harvard Law National Security Research Group, available at: www.academia.edu/526807/CLOUD_COMPUTING_and_NATIONAL_SECURITY_LAW (accessed 29 July 2019).

Jamsa, K. (2013), *Cloud Computing: Saas, Paas, Iaas, Virtualization, Business Models, Mobile, Security and More*, Jones and Bartlett Learning, Burlington, MA.

Lewis, J. (2002), "Assessing the risks of cyber terrorism, cyber war and other cyber threats", Center for Strategic and International Studies, Washington, DC, December, available at: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

Lynn, W. (2010), "Defending a new domain", Foreign Affairs, September/October, available at: www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain (accessed 30 October 2019).

NIST US Department of Commerce (2013), "NIST cloud computing standards roadmap", (Special publication 500-291 V2), available at: www.nist.gov/sites/default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf (accessed 2 May 2019).

OECD (2014), "Cloud computing: the concept, impacts and the role of government policy", OECD Digital Economy Papers, OECD, Paris, available at: http://dx.doi.org/10.1787/5jxzf4lcc7f5-en (accessed 12 December 2018).

Obama, B. (2009), "Remarks by the president on securing our nation's cyber infrastructure", Washington, DC., 29 May, available at: www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (accessed 18 July 2019).

Official Journal of the European Union (2019), "Regulation (Eu) 2016/679 of the European parliament and of the council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (general data protection regulation)", 27 April 2016, pp. 1-88, available at: https://gdpr-info.eu/ (accessed 20 November 2019).

Otava (2019), "Comparison safe Harbor vs the EU-US privacy shield", April 11th 2019, available at: www.otava.com/reference/how-does-safe-harbor-compare-to-the-eu-us-privacy-shield/

Park, J. and Park, J. (2017), "Blockchain security in cloud computing: use cases, challenges, and solutions", *Symmetry*, Vol. 9 No. 8, pp. 1-13, doi: 10.3390/sym9080164.

Paulsen, C. and Byers, R. (2019), "Glossary of key information security Terms – Revision 2", NIST US Department of Commerce, doi: 10.6028/NIST.IR.7298r2, available at: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (accessed 17 September 2019).

Schmitt, M. (2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, available at: www.ccdcoe.org/249.html (accessed 18 March 2019).

Šulovic, V. (2010), "Meaning of security and theory of securitization", Belgrade Centre for Security Policy, 5 October, available at: www.bezbednost.org/upload/document/sulovic_(2010)_meaning_of_secu.pdf

Tarry, S. (1999), "Deepening and widening: an analysis of security definitions in the 1990s", *Journal of Military and Strategic Studies*, Vol. 2 No. 1, pp. 1-13, available at: https://jmss.org/article/view/57850 (accessed 1 December 2019).

Terpan, F. (2018), "EU-US data transfer from safe harbour to privacy shield: back to square one?", *European Papers*, Vol. 3 No. 3, pp. 1045-1059, doi: 10.15166/2499-8249/261 available at: www.europeanpapers.eu/en/e-journal/eu-us-data-transfer-safe-harbour-privacy-shield

Tweneboah-Koduah, S., Endicott-Popovsky, B. and Tsetse, A. (2014), "Barriers to government cloud adoption", *International Journal of Managing Information Technology*, Vol. 6 No. 3, pp. 1-16, doi: 10.5121/ijmit.2014.6301.

US Department of Homeland Security – The President's National Security Telecommunications Advisory Committee (2012), "Report to the president on cloud computing, USA", National Security Telecommunications Advisory Committee, available at: www.dhs.gov/publication/2012-nstac-publications (accessed 13 February 2019).

Van Puyvelde, D., Coulthart, S. and Hossain, M.S. (2017), "Beyond the buzzword: big data and national security Decision-Making", *International Affairs*, Vol. 93 No. 6, pp. 1397-1416, doi: 10.1093/ia/iix184.

Wolfers, A. (1952), "National security as an ambiguous symbol", *Political Science Quarterly*, Vol. 67 No. 4, pp. 481-502, available at: www.jstor.org/stable/2145138?seq=1#page_scan_tab_contents (accessed 26 March 2019).

Zwattendorfer, B. and Tauber, A. (2013a), "The public cloud for e-Government", *International Journal of Distributed Systems and Technologies*, Vol. 4 No. 4, pp. 1-14, available at: https://online.tugraz.at/tug_online/voe_main2.getvolltext?pCurrPk=72462 (accessed 26 March 2019).

Zwattendorfer, B., Stranacher, K., Tauber, A. and Reichstadter, P. (2013b), "Cloud computing in E-Government across Europe", *Second Joint International Conference on Electronic Government and the Information Systems Perspective, and Electronic Democracy (Technology-Enabled Innovation for Democracy, Government and Governance)*. Prague, 26 August, pp. 181-195, doi: 10.1007/978-3-642-40160-2_15 (accessed 26 March 2019).

Further reading

Google Transparency Report available at: https://transparencyreport.google.com/?hl=ar

Maurer, T. and Morgus, R. (2014), "(Rep), compilation of existing cybersecurity and information security related definitions", New America, available at: www.jstor.org/stable/resrep10487 (accessed 29 November 2019).

Microsoft Law Enforcement Requests Report available at: www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

Privacy Shield website (2019), available at: www.privacyshield.gov/Program-Overview (accessed 20 November 2019).

Corresponding author

Hedaia-t-Allah Nabil Abd Al Ghaffar can be contacted at: hedaia2008@live.com