THE EMERGENCE OF LIMINAL CYBERSPACE – CHALLENGES FOR THE ONTOLOGICAL WORK IN CYBERSECURITY

Jukka Vuorinen
University of Jyväskylä
jukka.a.vuorinen@jyu.fi

Ville Uusitupa
University of Jyväskylä
ville.t.uusitupa@gmail.com

ABSTRACT

This philosophy-oriented paper examines cybersecurity and its ontological work in relation to spaces which are created by conventional perimeter security model and Zero Trust model. We argue that security works by a code of inclusion and exclusion, e.g., an individual user seeking access is either included or excluded in relation to the system. Therefore, cybersecurity divides the space through employing the code of inclusion/exclusion which directly affects the agency of users. We examine how the growing complexity of network environment makes information and cybersecurity to struggle with the simplicity of the inclusion/exclusion code. The simplified bifurcation is held by maintaining a strict order of the space for included users (i.e., how users and devices can behave once they are let in). Furthermore, we analyse the emergence of liminal spaces that contain both included and excluded actors. Liminal spaces, which have increased during the pandemic era, provide an intriguing spot through which security can be examined in terms of what it does, how it works out the ontological status (included/excluded) of its subjects.

KEYWORDS

Spatiality, Liminality, Ontological work, Zero Trust, User-centric Cybersecurity.

1. INTRODUCTION

Cybersecurity enables or halts users depending on whether the user is identified, authenticated, and authorised. In other words, the agency of the user depends on the decision of information security in terms of inclusion and exclusion. The bifurcation of inclusion/exclusion has spatial consequences. Cybersecurity divides the space between the inside and the outside. The former is the region in which the use of system takes place and is controlled and managed by information security policies, whereas the outside is mainly the unknown environment that has to be blocked (Vuorinen and Tetri 2012). This type of bifurcation can be carried out in different manners, but they still perform the same inclusion/exclusion code. The conventional perimeter security model, which develops security relying on the physical metaphors (e.g., castle walls, doors, see Weaver and Weaver 2008), has been criticised not being fit for the mobile or remote use of systems (e.g., Campbell 2020, Pieters 2011, Rose et al. 2020). Despite the "de-perimeterisation" efforts, security still works with the same code of inclusion and exclusion (insides and outsides emerge). The ontological work of cybersecurity – attempt to find out the "being" or "becoming" of user, what or who is that – differs in these different spaces. The challenge is thrown in by emergence the liminal spaces that are not exclusively inside or outside. For example, a user (authorized insider) can use their own device (unmanaged outside element) in the organisational network environment. In addition, working remotely from home (outside the local network of the office) refers to such a liminal space as well. The liminal space contains elements of insides out outside, which challenges the essential bifurcation of inclusion and exclusion – the crucial discourse and practice in the field.

In this paper, we analyse the significance of spatiality for cybersecurity. In the course of history, spaces and security have formed a significant pair. For example, the analysis of spatiality from plague towns to prisons and mobile controls can be found (Deleuze 2017, Foucault 2007a, 2007b). However, in the case of cybersecurity, space does not provide a place of internment, but it is a fluid and divisible space of transformation filled with different actors. The Covid-19 pandemic has changed the arrangement of spaces in which we work. Notably, the spaces – different sites of use – and data gathered from the sites, such as geolocation, IP address and timestamps, provide important information, which is used to separate the compliant users from the suspicious ones. We analyse space in liminal space in terms of ontology and two different cybersecurity models, the conventional perimeter security model and Zero Trust model. The latter has gained popularity in recent years and claims to tackle the information security problems relating to remote work although it increases complexity (Bertino 2021). We analyse the models in terms of "ontological work", which pertains to being and becoming. "What is an actor?" forms an ontological question that resides at the heart of cybersecurity. Ontological work relates to how an actor is identified and authenticated. What is the significance of space in this ontological work that defines the position of individual user? Importantly, we do not seek to determine which of the models is better, but we focus on the analysis of space and ontological work. By doing this, we can have a better understanding of the environment, in which the individual user seeking their autonomy acts.

We begin by analysing the essential information security code of inclusion/exclusion and its spatial ramifications. We examine the spaces that the code organises and analyse how these regions work. As we have explored the bifurcation of space, we analyse how the two security models treat their spaces. In addition, we describe the emergence of liminal – mixed – space that has become the dominating space for cybersecurity to operate in the pandemic environment.

2. BIFURCATION – THE IDEAL PURIFICATION OF SPACE

2.1 The Essential Dualistic Code

Information security is based on the idea of inclusion. A user who signs on to service goes through a process of inclusion. Inclusion pertains to the processes of identification, authentication, and authorization: who the user is, and what are the privileges given. With a chosen method, information security algorithms analyse whether a user is the one they claim to be. A username with a shared secret (a password), or a token that the user has (a mobile phone with a particular number, a key in case of a door), or what a user is like (a biometric fingerprint scanner) can be used for identification and authentication. This is the essential ontological work of cybersecurity (Vuorinen 2014; Vuorinen and Tetri 2012). Granting access to a system means that the user can go over a barrier – a door is opened. As the (virtual or physical) perimeters are crossed, the status of the user changes from an unknown outsider into a known insider. If a user is not identified and authenticated, then, of course, access is denied. This reveals the counterpart of inclusion: exclusion. Evidently, solely the particular users are let in while the other are excluded. This demonstrates the dualistic code by which information security works: allowed/denied.

The code follows strictly simple binary logic leaving no room between the digits zero and one, on and off, allowed and prohibited. There is no partial access. From the administrative point of view, a user is either allowed to see information or it remains disclosed. Surely, all modern information systems that are used by multiple users have different layers of security such as granular user accounts. Simply, for example, students at a university cannot access each other's accounts as the user accounts are isolated from each other. The accounts are parallel but simultaneously inclusive/exclusive. In addition, there are vertical user rights from a user to an administrator and a root, which can be organized different ways to create scalable layers of security (Hong and Kim 2016). Nonetheless, the code follows the same dualistic logic.

With the attempts to define or describe the dimensions of information security, the triad of confidentiality, integrity, and availability can be mentioned (e.g., Agarwal and Agarwal 2011, Dhillon and Backhouse 2001, Samonas And Coss 2014). The binary logic of the inclusion/exclusion method can be understood in relation to these terms. The confidentiality and availability procedures function in terms of inclusion and exclusion.

Integrity refers to the persistent form. For example, a file should hold its order (e.g., a hash) while being in storage – i.e., it should remain the same. If the file loses its order, becomes different, it is not secure or useful. In other words, it can be included (trusted) only if it holds its initial form – integrity. Otherwise, it is useless and becomes excluded.

2.2 The Code Divides and Cleans the Space

The fundamental dualistic code creates bifurcating spaces. Let us examine more closely what the spatial ramifications of the code are. At the ideal level, the dual category system (the code) bifurcates the space in which it is applied. In terms of information security, the ideal spatial consequence is a split of space into an orderly and controlled safe region of inside and outside that is a volatile, vibrant, uncontrollable, and possibly hostile exterior (Vuorinen and Tetri 2012). The outside is the (virtual/cyber) world of chaos that goes beyond the organised inside. Such divisions are not merely ideal but practical in some cases. For example, in perimeter security model uses information about location as a way of further inclusion (Weaver and Weaver 2008, Rose et al. 2020). If a user is within network perimeter, access can be given to all user resources within network.

Bifurcations go beyond security. "Inside" is defined by its order that springs from the desire of the holder – administrator, root, managers (Vuorinen and Tetri 2012). Insides and order are mundane. To clean a table is to exclude dirt. Mary Douglas (2003), a British anthropologist, makes a classic note on dirt; matter becomes dirt by its relation to other objects. For example, food on the plate is not dirt but as it falls on clothes, bedsheets, or on the floor, it instantly becomes undesired dirt. We want to emphasise that what is considered clean and dirty is defined by the desired order of the inside. In terms of information security, this means that inside is constituted on the inclusion of desired actors whether these were users, software or hardware. With regard to the desire and organisation, information security policies denote the desire of the organisation. All the actors and activities that are compliant with the policy are clean, proper and orderly. Cleanliness is based on the absence of noise. Noise can be understood in terms of systems here (Serres 2007), to a disturbing actor that distorts the logic of the system. This way, we can argue that information security threats are actors (e.g., hackers, malicious code, misuse of devices), that are incompatible with the order of inside. The danger is constituted by the position and effects that the threat actor would cause within. The actor can be harmless in another place – just as food on the plate instead of a floor.

The order of the inside is twofold. It concerns the relations of inside actors and, in addition their inner order (e.g., software and even thoughts of users). Firstly, the order pertains to the interconnective (and often spatial) arrangement of actors, including hardware, software, and users. Here, the question is of relations: which actors are allowed to connect, which actors can communicate and on which terms, which actors with specific parameters can read or/and write (see Rose et al. 2020). However, the order is also about engineering and managing the space in which the connections emerge. For example, using a desktop computer has spatial and virtual significance: where the system is used, which physical facilities are used, how they are cooled, how the power supply is protected. Furthermore, the specificity of locations allows hardware and software to be manipulated physically on the spot if such activity is needed. In other words, the order is about organising the relations of users, devices, software and data through a set of controls. Secondly, the order extends to the inner relations of these actors; each device is updated and made compliant, information security policies are imposed on users, the data is backed up. Staff can be rushed into security education programs. Here, we have arrived at the heart of security awareness campaigns that seek to grasp and influence the subjectively lived and experienced – phenomenological – world within the users. In terms of research, information security is compelled by the idea to make people behave in a particular manner (e.g. Alias 2019, Safa et.al. 2016; Vroom and von Solms 2004). It and its controls are employed to serve the desire of the organisation. However, simultaneously the organisation is bound to feed the security machine that consumes the energy of the system (Vuorinen and Tetri 2012).

3. SPACE AS A PROVIDER OF CERTAINTY

The constitution of an orderly inside seeks to gather spatial information. Spatial information refers to the firm knowledge of and about the space used. For example, spatial information can be developed as a part of

situational awareness. For example, in a controlled environment – such as a well-managed facility for using IT resources – it is possible to gather data about the ordinary network traffic – where the packets travel, with what frequency, from which points – and then to define the baseline of that activity. This way, the order of the inside is made visible. The baseline describes the tempo-spatial rhythm that the users and devices with their routines create. It anticipates the future in terms of what to expect what it should be like and provides a canvas against which to compare all the future traffic. Baseline describes the cosy rhythmic hum of the inside that can give a warm and fuzzy feeling of security. If there are deviations, then flags rise. This provides an opportunity for further analysis of the case. The outside, on the other hand, is beyond control. Indeed, the external network can be probed, and information of situational awareness can be shared between trusted parties, but it cannot be managed. In terms of the inside, the perimeter is the surface of contact towards the outside; by analysing it, something of the outside can be known, but it cannot be captured entirely. In other words, the outside environment is too large to be known. Security establishes the bifurcation by organising the inside in the most impeccable way possible with the current resources. Inside stands out because of its order.

The rich knowledge of the site creates spatial certainty that brings about stability. When the baseline is known, it can be used as a tool of identification. At least in the conventional perimeter network security architecture, the company network space works as an identification. For example, inside resources are accessible for users in the company network IP-address range. An IP address is not a bullet-proof method of identification. However, in addition to IP, all the signals that the user emits directly or through the side channels provide partial evidence. Likewise, hiding such information makes the identity disappear. The anonymity of Tor-network is partly based on the fact that every user looks similar; no uniqueness can be extracted. In a conventional company network, user behaviour and familiar signals do not matter in terms of trusting in the user's identification as it is the filtering system at the perimeter that is trusted. In other words, when ordinary user behaviour is known, it can be used as supporting evidence of identification. It should be noted that information security is interruptive by its nature (Vuorinen & Tetri 2012). Security procedures tend to interrupt the user (or the system) and give order words: place the finger on the scanner, give your credentials, restart the machine to update it. The baseline makes information security quieter and more unintrusive. It can hold the identity of a user without asking it constantly if the environment is controlled. The routine activity can be used as a part of the continuous authentication of users.

Spatial stability – working at the same site with the same devices – makes it possible to employ more controls. A stable environment provides certainty about the space, as the resources can be accessed, analysed and managed with group policies, which can be in a social (discursive) or software format (group policy). The more controls there are or more the stability of the environment is trusted, the more the order is strengthened. We have described an ideal case of the inside. Ideally, it is known and dominated by the desired order that establishes the difference between the system and its external environment. However, in practice, the insides are filled with movement, distortion and noise. There are dark corners within. Moreover, devices fail, and users do not comply. Notably, the inside lives on the resources of outside. There is no energy within – everything has to be imported inside. This is aligned with the general system theories: The systems (also social systems) differentiate themselves in relation to their environment (Luhmann 1989). Thus, the inside is merely reorganised and controlled outside (see also Vuorinen & Tetri 2012). The users are outsiders that become insiders through the filtering process. The devices can include dirty firmware. Updates can be buggy. In addition, a device can be entirely managed, but certainty about user's identity can be questioned through user and entity behaviour analytics. Constantly, the outside is within the inside region, but the exterior is present in the form of resources that are put in order and arranged according to policies. Information security policies are probably imported as well. Nonetheless, organisations are used to dealing with such import procedures.

Hitherto, as we have described "inside" as an orderly and controlled space, we have referred to it as an ideal type in the field of information security. How the goals of information security are achieved is a different question. Security is never about control of everything, but its target is limited: the confined inside region. All the security measures seek to establish and reinforce the division between inside and outside. The security methods seek to prevent the external actors from accessing the system in the first place – "keep the dirt out". However, the practitioners that fight the security threats probably agree with Michel Serres's (2007, 86) argument of work "is a struggle against noise", but noise always finds its way within. Thus, it is important to know whether there the system is safe or compromised – "yet, look for the dirt within".

Zero Trust holds that “there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)" (Rose et al. 2020, ii.) Currently, it seems that practitioners are keen to be careful and assume that systems are infiltrated. In terms of bifurcation, dirt is already within. Importantly, in all the above cases (whether the inside is trusted or not), in case an external actor is found, it is sought to be removed, excluded. It always comes down to “authorized and approved subjects (combination of user, application (or service), and device) can access the data to the exclusion of all other subjects (i.e., attackers)” (Rose et al. 2020, 4). In simple terms, purity is sought. Thus, bifurcation has become a dominating idea of security, in a sense it is a trope that is recognisable in security seeking environments. The trope is present in the field as metaphors of castles (e.g., Weaver and Weaver 2008), but also in the terms such as green zones (a safe region surrounded by a more uncontrolled space), the cyber kill chain (Lockheed Martin’s terminology) which underlines outside region as a source of advanced persistent threats. The bifurcation is present in every firewall and login procedure; they establish the inside and outside.

Although the binary code of security and the bifurcation make it possible to think in terms of pure/impure, safe/contaminated, the Zero trust paradigm implies that the practical securing work does not use such binary thinking in such a way that the inside would be trusted by default. This is because the paradigm assumes that the attacker is already present in the inside region. The inside is seemingly in order but on basis of that order no trust is build. The inside means nothing in terms of trust as “an enterprise-owned environment is no different—or no more trustworthy—than any nonenterprise-owned environment” (Rose et al, 2020, 1). Instead, it is about risks which refer to the possibility of an incident and the severity of lost or damaged assets (Pieters 2011). Risk varies in terms of a threat, a system and an asset. For example, to lose a mundane shopping list is quite different from losing a social media account that brings food to the table. The risk involves unknown, even unthought and differs from the dualistic code. Risk is a continuum. It can increase or decrease.

Overarchingly, to form our argument at a more abstract level, we conclude that this struggle against actors that are incompatible with the order of inside – struggle against impurities – is, in fact, ontological work which requires resources. This is to say that the questions of being and becoming have to be answered. For example, an actor that behaves inconsistently becomes suspicious. An ontological question arises: what is that? Can it be a threat? What can it become? In other words, is that dangerous, i.e. incompatible with the inside order? As this work of finding out the “real” being of the actor requires work, there are two different strategies to spare resources. The conventional network architecture deals with the ontological work at the border of the system. To filter – for example, asking credentials – is to work with the question of ontology. As the filtering process is completed, users can be given further security privileges within the organisational network – i.e., user becomes inherently trusted after the filtering process. However, Zero Trust paradigm assumes users to be compatible with the order temporarily. An insider is an insider as long as new privileges are needed or something violating the baseline occurs. For example, by authenticating successfully to a service the user is temporarily verified as an insider. Yet, if the same user proceeds to download an excessive number of files, which is considered as a deviation compared to the baseline, then the user might be forced to authenticate themselves again and prove they are still the same insider they claimed to be before. The ontological question, what is that, needs to be answered. The verdict comes in the dualistic form but the ontological work behind the verdict is about probability and risk. In other words, ontological work seeks to find out what an actor is and then translate it on the level of binary logic (threat or not).

4. THE PANDEMIC AND SPATIAL UNCERTAINTY

The covid-19 pandemic has changed the working environments, as organisations have shifted to the mode of remote work. Indeed, this is a significant change from the information security point of view. The users are no longer in the gentle embrace of an office environment that would enable the use of managed devices in a sensorrich environment. Instead, the insiders are out there in the volatile exterior. In terms of inside/outside binary, the users are in a liminal space; out there in a suspicious environment but not yet totally out of control. Control is partly lost as the signals of behaviour fade into the depths of the outside world, which baselines cannot capture. The canvas of comparison has been torn into pieces. More importantly, diminishing spatial control means losing spatial certainty that no longer translates into ontological certainty.

Consequently, a question arises: how the problem of uncertainty is solved? The answer seems clear, as more ontological work is obviously done. However, this time the inner space is not available for analysis and the outside space is too vast and general; thus, the user and the device in use becomes the subject of analysis. The analysis itself is ontological work; it seeks to banish the suspicion. In Zero Trust environment that suspicion is aroused constantly.

The loss of control and change in space adds a new mixed code parallel to the conventional binary code of information security. The space of security becomes a liminal space that mixes inside order and outside elements. In Table 1 we have described the contradictory logic of liminal space and how the models react to it.

Table 1. Spatiality, models, and ontological work

Spatial dimension	Actors	Ontological work at the level of inclusion and exclusion	Ontological work carried out in Perimeter security model	Ontological work carried out in Zero Trust Model
Outside	Chaotic actors, hackers, malicious code, but also useful resources, and insiders that have logged out.	Actors need to be defined in terms of combability with the inner order. The insider users and compatible software needs to be recognised and allowed access (availability). Other actors must be excluded (confidentiality).*	Outside is not trusted – sought to be excluded.	Outside is not trusted – sought to be excluded.
Inside	Authorized users, devices and other resources	Users and devices that must be kept in order in relation to the information security policies. Insiders must be enabled to work, to achieve the goal of confidentiality, integrity, and availability (CIA). **	The insiders are enabled at the perimeter. Once actor is within the ontological work can be delegated partly to the spatial location. All the actors that have passed the perimeter check are trusted.	The insiders are trusted only in momentary manner. Microperimeters and continuous analysis of user behaviour and context becomes the basis of categorizing users to insiders and outsiders. The privileges cannot be inherited from borderline control i.e., treats inside as an outside.
Liminal; mixed inside and outside	Authorised users (insiders) reside in uncontrolled spaces such as homes and using unmanaged devices. Cloud services, legacy IT and Shadow IT.	The same as * and ** above.	The model has difficulties in dealing with unmanaged devices. The only possibility is to extend the office base into the outer world through trusted gateways. It cannot handle “use your own device” requirement. Ontological work is increased at the border – e.g., multiphase authentication.	Works in the similar manner as above: as if users and devices were constantly coming inside from outside. Constant Re-checking.

For sure, the shift in the pandemic era has not been such dramatic as it may seem. Firstly, cloud services have been widely used in modern organisations before the covid. Perhaps, remote work opportunities were not utilised with such volume as in lockdown periods, but the option for such a way of acting was available. This means that the pandemic did not create new problematisations but rather it emphasised and boosted some problematisations. For example, the Zero Trust security model promotes constant ontological work as it promotes doubt and paranoia in the form of continuous checking on the identity of the user. It means that there is no permanent inside, but an insider status is only given temporarily. The inside is certainly organised orderly: security policies are applied, and insiders are granted access. However, spatial or temporal trust is not inheritable in Zero Trust paradigm (Rose et al. 2020). Trust fades away with time and spatial changes. For example, a certain period of passivity or a change of IP address is considered suspicious. For a user, working in a Zero trust environment is a constant becoming of a trusted user. Indeed, information security is

considered a process (making of security) in a conventional network security context. Still, Zero Trust rejects "being" – the stability of status – and embraces becoming, which refers to vanishing trust. Trust is momentary; multifactor authentication is temporary. Zero Trust is about continuous renewing and rechecking. The continuous process reminds of Gilles Deleuze's (2017) description of control society. There are no places of rest, there is no final destination; everything is mobile; there are no specific spaces for controls, but they are everywhere. In a disciplinary society, on the other hand, there are particular spaces of surveillance and control, which are limited spatially and temporally.

In the pandemic era, some organizations have had the urge to stick with high control without compromises. For example, if an organisation is dealing with sensitive data, maintaining a high level of control can be a top priority. In these cases, the spatial inside space becomes stretched, which leads to the question of information security topology. The inside space is merely extended into the homes. This means, for example, solely using strictly controlled and managed devices with secured connections. In the pandemic environment such a requirement is recognised in the field (Bernard &Nicholson& Golden, 2020). The office moves home and works over VPN. However, there cannot be total control over, who is using, are the home office doors locked and computers locked. This of course has a decreasing effect on spatial certainty which emphasises the position of the user again. In a sense, users are simultaneously inside and outside. Zero trust framework treats the inside space in the same manner: as if outside actors were within the organisational space all the time.

The cloud services are used on daily basis in various organizations. There are different cloud-based services from infrastructure to software, but all of these outsource – partly at least – information security management. While the services can be administered and managed in a restricted way, physical access to the infra is out of the question. Cloud services are not within an organization, but neither they are outside. Being partly controlled by a trusted third party these services lie in a third space beyond inside and outside, i.e., in the liminal. An example of cloud services in the liminal space approaching the chaotic outside is the so-called Shadow IT, typically the cloud storages and other SaaS used by organizations' business departments or individual users without the consent and management of the centralized IT and security functions.

An intriguing example is yet to be provided by legacy IT that is found problematic in the field. Legacy IT is outdated machinery that cannot be updated to meet the current standards. Now as seen above the covid pandemic has turned the organizations and users to move towards the outside, taking a position in the liminal space; slightly out of control yet able to hold some sort of recognisable order. The legacy IT cannot transform itself into the liminal space but stays an outside element even in a controlled environment. Initially an insider slips away as the space changes and slowly it becomes an incompatible element with the inner and desired order. It has become a threat.

5. CONCLUSION

An individual as a user is subjected to the ontological work of information security, which seeks to answer what the user is and eventually decides whether the individual should be allowed to use the system in the requested way. In other words, information security affects the agency of individual users. In practice, information security is bound to work by the dualistic code of inclusion and exclusion. Consequently, the code bifurcates space into inside and outside regions. The former is sought to be organised orderly by the desire of its owner. The latter, on the other hand, is out of control in the sense that the chaotic outside world can be observed but cannot be managed. If a system were totally isolated – without a connection with the outside – maintaining the order of inside could perhaps be uncomplicated. However, the inside region requires outside as a resource pool from which to draw energy. This is to say that the two sides, almost always, are in connection with each other. Security requires energy. However, it turns that energy into the form of interruptions as it works ontologically (e.g., a requirement of credentials is an interruption). To save energy and to avoid unnecessary interruptions, the bifurcation of space can be harnessed for ontological work. Thus, to answer the problem of inclusion and exclusion, the perimetric network security model inherently trusts (includes) all the users within the organisational network. E.g., spatial information such as an IP address can be used as a tool of authentication. In other words, the perimetric network security model trusts the filtering system that resides at the borderline and gives privileges for everyone within the perimeter.

However, if the connections between the inside and the outside increase and gain strength, liminal spaces, which mix outside and inside elements, emerge. The liminal spaces become significant in terms of information security as they defy the dualism of the code by which security works. In simple terms, the liminal spaces distort the spatial order of information security. Therefore, it also makes harnessing spatial information for ontological work difficult. For example, if a user is not inside the perimeter, then using that information for inclusion/exclusion decisions is impossible. With the rise of remote work – and the covid-19 pandemic made the remote work common practice for a number of organisations – the liminal spaces have become dominating form of information security space. Zero Trust information security model transforms the topology of information security. The space is still divided between inside and outside, but now there are spots of inside scattered around the outside. Secured gateways connect the inside to the spots, but these liminal space actors are trusted only momentarily. This means that the ontological work has increased; thus, the subjects are more likely to be interrupted. Or they do not have the option to move inside the space that would be trusted. In terms of the autonomy of an individual, in Zero Trust model, the conditions that make autonomy possible are questioned more frequently.

REFERENCES

Agarwal, A. and Agarwal, A., 2011. The security risks associated with cloud computing. *International Journal of Computer Applications in Engineering Sciences*, *1*, pp.257-259.

Alias, R.A., 2019. Information security policy compliance: Systematic literature review. *Procedia Computer Science*, *161*, pp.1216-1224.

Bertino, E., 2021. Zero Trust Architecture: Does It Help?. *IEEE Security & Privacy*, *19*(05), pp.95-96.

Campbell, M., 2020. Beyond zero trust: trust is a vulnerability. *Computer*, *53*(10), pp.110-113.

Deleuze, G., 2017. *Postscript on the Societies of Control.* Routledge, Abingdon.

Dhillon, G. and Backhouse, J., 2001. Current directions in IS security research: towards socio-organizational perspectives. *Information systems journal*, *11*(2), pp.127-153.

Douglas, M., 2003. *Purity and danger: An analysis of concepts of pollution and taboo*. Routledge.

Foucault, M., 2007a. *Discipline and punish: The birth of the prison*. Duke University Press, Durham.

Foucault, M., 2007b *Security, territory, population: lectures at the Collège de France, 1977–78*. Springer, Heidelberg.

Hong, J., Kim, D. 2016. Towards scalable security analysis using multi-layered security models. Journal of Network and *Computer Applications*, 75, pp.56–168.

Luhmann, N. (1989) *Ecological communication.* University of Chicago Press, Chicago.

Pieters, W., 2011. Representing humans in system security models: An actor-network approach. J. *Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, 2(1), pp.75-92.

Samonas, S. and Coss, D., 2014. The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

Safa, N.S., Von Solms, R. and Furnell, S., 2016. Information security policy compliance model in organizations. *computers & security*, *56*, pp.70-82.

Serres, M., 2007. *The Parasite*. Minnesota University Press, Minnesota.

Vroom, C. and Von Solms, R., 2004. Towards information security behavioural compliance. *Computers & security*, *23*(3), pp.191-198.

Vuorinen, Jukka. Parasitic *Order Machine – A Sociology and Ontology of Information Securing*. Annales Universitatis Turkuensis, Turku (2014).

Vuorinen, J. and Tetri, P., 2012. The order machine–The ontology of information security. *Journal of the Association for Information Systems*, *13*(9), pp. 695–713.

Weaver R, Weaver D., 2008. *Guide to tactical perimeter defense: becoming a security network specialist*. Thomson/Course Technology, Boston.