Understanding HSE implications of remote work through a digital complexity perspective

T.O. Grøtan

SINTEF Digital, Trondheim, Norway. E-mail: Tor.O.Grotan@sintef.no

Digitalization and increased use of remote operation is a growing trend in the Norwegian petroleum industry. Substantial amounts of work that previously had to be done on an offshore facility, can now be conducted onshore. This paper presents a specific part of a study (Bodsberg et al., 2018) funded by the Norwegian Petroleum Safety Authority on HSE (health, safety and environment) implications related to cyber security in remote operation of oil and gas installations. The scope is focused on digital technology that supports, controls and monitors industrial production and safety functions (also denoted operational technology - OT), thus not addressing general (administrative) information technology (IT) in full.

A purpose of the study was however to draw a bigger picture regarding; implications for employees and changed framework conditions (contracts and hiring); increased complexity in the form of increased (digital) interaction; increased vulnerabilities and greater demands for ICT security in specific solutions; potential dilemmas between organizational security vs. ICT security.

The analyses of the empirical material were partly based on an analytical framework on digital complexity drawing on Grøtan and Albrechtsen (2008), which comprise

- An approach to complexity that recognizes that organizations are undergoing continuous change, that the dynamics of change are relational, and with an emphasis on continuous balancing of human, technical and organizational conditions (HTO balances)
- A description of two different but related forms of HTO balance; 1) the balance between primary work (work process) and secondary work (work form), and 2) a shift in foreground and background of the value creation process, so that value creation is more linked to interfaces between organizational units, rather than within units
- A perspective on digital technology as a facilitator and carrier of a "hyper-reality" where technical and social systems and components, at the forefront, are represented predominantly based on their ability to reconstruct the whole for various and changing purposes

The paper describes this updated analytical framework, an assessment of the value of applying it on the empirical material available, and some conclusions that can be drawn from this specific part of the analysis.

Keywords: Remote work, digital complexity, HSE implications

1. Introduction: Increased complexity

Complexity is a term that is tempting to use when uncertainty prevails. However, it is also difficult to define. For a long time, complexity has been a catch-all concept with many meanings and that has been used in numerous ways.

One of the most common approaches to defining complexity is to point out the opacity that arises when the number of actors / components, and the number of connections between them, increases greatly. The tendency in recent scientific approaches, e.g. actor-network theory, is to diminish the difference or reformulate the relationship between the human and the technical. This, in turn, also helps to make it more obvious to designate such systems as "complex" (i.e. difficult to grasp or incomprehensible in the lens of traditional frameworks of understanding).

Remote work, also denoted telework, definitely belongs in this area, not least because the capabilities of the digital technologies that it rests on are (constantly) dramatically changing and expanding. A few years ago, we were concerned with secure data transfer from A to B, today we are keen to take advantage of artificial intelligence (AI) which in many people's opinion can dramatically change (HTO) rules of the game. Yesterday's perceived "complexity" is therefore modest compared to that of today's or the future's technology. It is becoming less relevant to point out that digital technology is merely about separating and juggling with zeroes and ones at a spectacular pace. Although the statement is not incorrect, it practically does not say anything about the implications of e.g. telework with today's technological status and prospects.

Nevertheless, questions can always be asked as to whether the lack of transparency should be described as complicated or complex. One should keep in mind that a complex system is not only difficult (complicated) to model or explain; the

Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0

term "complex" should be reserved for systems where it is expected that the insight into, and knowledge of, the system's behaviour is volatile, that the system per se is in motion and thus may have changed before one has finished modelling, or otherwise understood by one limited event or behaviour. That (technical) systems are constantly changing or being updated without everyone – or perhaps anyone – overlooking the consequences is one important side of this, but it also comes with a complexity having a holistic premise. The HTO system as a whole can be more than the sum of the parts, and that "more" can turn out both positive and negative in relation to acceptable intentions and expectations. Accordingly, a system referred to as complex can also be expected to be self-organizing, in the sense that new behaviours or patterns of interaction may arise without the design or intention from a "governing" or "responsible" actor. The degree of complexity need not be constant either. Nor it is not unreasonable to assume that a specific system for example can "commute" between complicated and complex, depending on the circumstances (Kurtz and Snowden, 2003).

However, it is difficult, if not to say impossible, to locate, grasp or manage "complexity" as an independent or tangible phenomenon. The present approach to complexity is therefore more about accepting the premise that the seemingly understood and stable is changing, that insight and understanding can have a volatile character, that behaviours can change both imperceptibly and suddenly/radically (as a so-called discontinuity), and that these characteristics occur within a time horizon that requires them to be taken seriously in daily life, not just as a remote or exotic opportunity of sheer academic interest.

Complexity is thus not something that arises with telework. It is more a premise one (eventually) chooses to accept, and thus prepares to understand and handle the implications of. But such an acceptance would be directionless and to some extent meaningless if it is not accompanied by an interest in which conditions can generate complexity or affect the "intensity" thereof. In that respect, the main angle of the study this paper draws on (Bodsberg et al., 2018), is to focus on relational aspects. This is in line with recent research on interorganizational complexity and safety in the petroleum industry on the Norwegian continental shelf (Milch 2018), where it is recommended to emphasize quality relationships between union workers in various companies and long-term, trust-building relationships between middle managers to counteract inter-organizational complexity. This is also in line with recent research on crisis complexity (Johannesen 2017), where the focus is more on "Complex Responsive Systems/Processes" than the traditional focus on "Complex Adaptive Systems".

A key question will therefore be whether and in what way ICT and teleworking contribute to, or influence (the complexity in/of) important relationships related to, e.g. the operation and management of operational disruptions, or the modification and maintenance of critical industrial ICT systems.

One way to address relational aspects is to focus on (presumptively fragile) HTO balances and equilibria to understand collaboration in an "Integrated Operations" (IO) context, as was done by Grøtan and Albrechtsen (2008)). Such an approach will not be about finding and protecting a single critical HTO balance, but addressing several simultaneous balances in different but overlapping (ecological) niches of interaction that include telework. Each of these is expected to be in a dynamic equilibrium, where an equilibrium is the result of continuous adaptation.

In the following, I will focus on two different perspectives on such HTO balances, which can help to illuminate the potential complexity of interaction involving remote access and telework.

Basic HTO balances: Primary work, secondary work, articulation work and common forgetfulness

The first and basic HTO balance is about understanding and taking into account the relational and social nature of the collaboration. This is pointed out by Hepsø (2006) who, in the context of IO, encouraged the industry to be more aware of social and relational conditions that contribute to robustness in organizational interaction. Hepsø takes a distinction between primary work and secondary work as his point of departure and argues for a balanced integration of these. In short, primary work is the activity that directly addresses specific agendas and goals in a given work situation, and which is thus also the primary basis for identifying a set of activities in a chain of interaction. When several activities intervene, this can be called an interaction matrix. All work that comes in addition to the primary work to make the primary work feasible, including reorganization and maintenance of the chain or matrix, is called secondary work.

A special variant of secondary work is articulation work; the essence of this is to unite and reconcile incompatible assumptions and procedures in the absence of relevant standards/procedures that can be "imposed" on the parties. The articulation work is characterized by the fact that it solves inconsistencies by packing up compromises that "get the job done", which solves the situation locally and temporarily so that one can move on. Such "closure" is about creating unity, but this unity can also be about ignoring something that cannot be resolved otherwise. If, or when, the articulation work is not represented in the job descriptions, it will be difficult to analyze the actual ongoing work. For this paper, the implication is that if teleworking is to be understood as something more than individual actors' use of technology, then we must try to understand the actors' joint construction and integration of primary work, secondary work and articulation work, fundamentally understood as HTO balances.

The claim that articulation work may also require or lead to "common forgetfulness" may seem unfamiliar but resonates with historical roots in safety research, formulated long before today's ICT solutions and prospects were relevant. For example, with reference to Barry Turner (1978), Karl Weick wrote in 1998 that "organizations are defined by what they ignore – ignorance embodied in assumptions – and by the extent to which people in them neglect the same kinds or considerations" (Weick 1998). This is an important counterpoint to more common organizational understandings, where one intuitively seeks solutions for "common knowledge/ situational understanding" and the like that supports the primary work in a direct and instrumental way. If the understanding of secondary work is too unilaterally directed to this one melody, creating common denominators that "everyone" understand in the same way so that the primary work slides more easily, one is also at risk of overlooking something essential at the inter- as well as the intra-organizational complexity; namely that the binder (secondary work) may as well be common forgetfulness, as common references. The underlying phenomenon of "variable disjunction" among collaborative parties is probably inevitable, even with "infinite" access to information – and maybe especially then.

In relation to the social and relational nature of telework, there is thus a risk of underestimating something that is both potentially dangerous, but also a possible strategy for improvement. If Hepsø, Turner and Weick (and many others) are right, then the industry (and many others) have long traditions for ignoring a source of complexity. That is, the need for articulation work, including that this can manifest itself as a "common forgetfulness" which camouflages "variable disjunction". This tradition has existed long before ICT / teleworking was recognized as a challenge in the way used in this paper.

It is now a high time to raise such perspectives, and Hepsø's (2006) submission of this is still a good starting point for moving forward, both to understand the underlying contribution to inter- as well as intra-organizational complexity, and the potential contribution to increased robustness and resilience that articulation represents in terms of supplementing the "main melody" of primary work. In this sense, the secondary work is a counterpoint to the primary work. At the same time, the articulation work itself contains a counter-punctual element in the form of "shared forgetfulness" that runs parallel to the efforts to create common references that legitimize "closure".

Important questions are how such a balance can be created and maintained when remote work is included, how it can be affected, lost or displaced. Will teleworking be able to influence articulation work towards common explicit references or common forgetfulness, or will it just be able to support an attempt to eliminate the need for articulation work by strengthening primary work?

Hepsø (2006) focuses on how shared information objects are created through dialogue in which they try to understand each other across subject and professional boundaries ("perspective making" and "perspective taking"), and employ the term "boundary objects", i.e. objects that function as more or less automated "translators" between interacting "species" or actors within an interaction niche. Formal representations of knowledge (computer models, formalized information structures, "dashboards") can however in principle never become shortcuts for creating such boundary objects and are therefore not sufficient basis for decision-making without associated articulation work. For boundary objects to work, there must be room for active negotiation and arbitration of meaningfulness around these objects, and the articulation work is in itself a "balancing act" that is sensitive, among other things, for whom to participate and which relationships they have from before. It goes without saying that a "digital nomad" will meet special challenges when he or she is sporadically involved in such processes. Furthermore, a seemingly well-functioning boundary object, which the players rely too much on, could be dangerous. Studies should therefore be aimed at understanding whether, and how, stakeholders develop mechanisms to deal with obviously inconsistent ICT systems and infrastructures, but also whether or how they are able to identify the less obvious needs for such mechanisms and strategies, when the situation requires this.

Hepsø (2006) also points out that there is a fundamental connection between articulation work and trust. Moreover, he shows that the building up of trust and obligations in different situations are complex processes in themselves. This derives important questions such as: What is "primary work", what is "secondary work", and what is "articulation work" for establishing and maintaining trust and commitment in remote work where actors are separated in time and space?

So far, we have described ICT solutions (for remote work) as something advanced and complicated that is "passively" available for use in work processes, and which is part of an HTO constellation where it is mainly the human and social component that causes the overall socio-technical to move, e.g. between complicated and complex. I am not going alter this position and thereby add an excessive intrinsic complexity to the technology per se, but I will nevertheless point out that this HTO interaction can be or become even more intricate and complex than what we have described so far. Indeed, ICT can also be understood as a *re*-presentation technology (Grøtan, 2007), which creates new conditions for mastery and control in a complex system. ICT thus channels a new form of power in which reality is replaced or supplemented by a "re-presented" and constantly re-organized understanding of reality. Such a "hyper-reality" is attractive because it can be changed continuously based on prevailing/changing goals and intentions. Such an ICT perspective may signify that we have to reformulate terms such as "rich vs poor information channels" radically, and it also complicates the understanding of what Hepsø refers to as "perspective making/taking" and boundary objects, including trust and obligations related to them. Will the response be a more active meaning-arbitration and negotiation process carried out as articulation work, or a capitulation to the "superpower" of re-presentation and thereby cause a more amputated articulation work?

Another, close perspective is to look at the ever-increasing production of information as a self-propelled spiral that supports a "garbage can" decision-making process rather than a process with a clearly defined goal and meaning. Grøtan (2007: 84) summarizes this with that:

- Information is both
    - a description of, and a reference to, conditions and relations in a given reference area, but also
    - self-referencing, i.e. a relationship to other, previous descriptions within the same domain. Existing information thus "produces" new information when combined with "fresh" information
- The ability to interact between modern, standardized ICT infrastructures dramatically increases the combination possibilities
- The information is perishable and can be easily replaced. The content of the information – the news value – is by definition a transient and perishable result. Impaired information content must constantly be compensated through updating and reproduction

This decade-old description of the information spiral can be read as a paraphrase of what we expect from artificial intelligence (AI) today. However, the information spiral reflects a relatively "blind" human and organizational news appetite, where the possible and accessible takes precedence over a planned and careful selection process. Today's expectations of AI are, in comparison, more marked by a notion of something "magical" about technology itself. In any case, we cannot overlook that an "overproduction" of information, with or without an intelligence stamp, can affect both primary and articulation work, and not least the balance between them. One can already see trends in the use of large amounts of data and the use of machine learning as an argument for reducing the focus on models and hypotheses on how systems work. If the primary work is "computer driven", what will the articulation work be about? Will the premise of complexity be "forgotten" through closure just as described by Weick (1998)? Will this also lead to less negotiation and sense-making, and thus more amputated articulation work?

A critical question that can and should also be highlighted is where and how "real" HSE issues are understood, described and taken care of in a context where articulation work is an important (and recognized?) supplement to primary work. Will HSE as a phenomenon be, or is it already, taken as "hostage" and described exclusively in "primary meaning"? How will HSE in telework be specified and described?

Organizational foreground and background, mixed knowledge regimes

Another potential source of an HTO imbalance is a (then expected) shift between what is foreground and background in decision-making (Sørhaug 2004). We have become accustomed to seeing the organization as a "decided world" in the foreground, while other actors/partners and thereby the interfaces to these form the background. The trend is now that labour and capital flow through the companies, with the interfaces as the foreground. With digitalization we can accelerate a development where value creation takes place between the units, not in them. Value creation, not the units, is the constant of such an equation. Inter-organizational complexity (Milch 2018) is one of the implications.

Another key to understanding these issues (also in the interfaces) is the concept of mixed knowledge regimes, which are based on a clear distinction between (professional) discipline, managerial line and network (Sørhaug, 2004). There are signs that the network dimension is on the rise, but that also carries a clear premise of the necessity of shifting and moving compromises between these dimensions.

Important questions are whether such shifts are reflected in the conditions for and execution of teleworking, individually and collectively, specifically whether this affects primary work and articulation work, and the balance between them. Where, and by whom, are the criteria for successful interaction defined in the interaction matrix, within or between the businesses, and can we see traces of "moving compromises" in this? Have (the new) "ecology" of actors changed, who are the dominant "key species"? To which degree is "the network" a prominent player in itself?

It is also of interest to know how such changes are reflected in the organization of HSE work. Knowledge is the new capital, companies use knowledge to rationalize knowledge, not just to rationalize processes. What/where is HSE when knowledge is used to rationalize knowledge?

Increased vulnerabilities and greater demands for ICT security

Increased ICT dependence can be expected to lead to stricter requirements for ICT security. However, much indicates that there is a considerable backlog in industrial ICT security, also in areas that are targeted by teleworking. New attack vectors and surfaces are emerging with increased digitalization in industry and society. A. Bochman (2018) of Idaho National Labs in the US describes the limits of state-of-the-art "cyber hygiene" very clearly, arguing that "*no investment in digital defenses can protect critical systems from hackers*". The motivation of the threat actors that may exploit vulnerabilities are also changing dramatically. According to the Washington Post, Greenberg (2019) offers a "*hair-raising, cautionary tale about the burgeoning, post-Stuxnet wold of state-sponsored hackers*".

Telework encompasses both generic IT and OT, and this combination presents special challenges in terms of different technology, languages, and culture. The implications of this are very important to understand for any attempt of framing the cyber security implications of telework.

Experience with cyberattacks against industrial plants and critical infrastructure thus suggests that the industry must prepare for a wide range of threats, from spurious and incidental occurrence of malware and opportunistic hacking activity, to (criminally or politically motivated) intelligence gathering and mapping over time, with an intention of developing capabilities for orchestrated and deliberated attacks, even towards safety critical systems specifically. Increasing the scope of telework may provide new opportunities for those seeking to disclose operational vulnerabilities, e.g. as part of the preparation for an attack.

Furthermore, the Internet is an intelligence arena without national borders (and without any Geneva Convention or other supranational, legal/ethical frameworks). Renowned experts have recently expressed concern that someone may "turn off Norway" digitally, while the former head of Europol is concerned that state actors are joining criminals online.

Seemingly trivial digital behaviour has gained tremendous value in a digital economy, where the very business idea of the major players is to collect as much data as possible about users, their activities and opinions, and where virtually no detail is too small. This "business to consumer" oriented and systematized collection, monetization and commodification of vital as well as surplus data from nearly all life arenas has been coined "Surveillance Capitalism" by Zuboff (2019). It must be expected that the very same ideas and models find fertile grounds in the "business to business" arena. The industrial parallel to this may be that through large-scale data acquisition, it will be possible to find interesting patterns across a wide range, for industrial applications and disruptive business models, e.g., utilizing digital twins, for HSE purposes, but also for economic, financial or political gain. This applies not least to the use of "big data" and "artificial intelligence" to observe and analyse behaviour, phenomena and trends, with completely different levels of ambition than previously imagined. BBS (Behavior Based Safety) may be given an opportunity for revitalization, but the very same insights can easily be "weaponized" for unfriendly purposes. Surplus information in the wrong hands may thus create new vulnerabilities, e.g. related to smart metering systems in energy supply (Grøtan 2018). On this background, we should assume that also telework will be enrolled into complex landscapes of threats and vulnerabilities that exceed most of what has previously been prepared for through ICT security.

The consequences of disrupting control processes in a subtle way were made visible through (the first) famous Stuxnet attack, where some actors, over a relatively long period of time, could confuse operators and process control by manipulating the values of the measurements. Commercial and political influence through digital communication has become a very relevant topic during the past years. Decision makers in the industry can also be designated targets for such influence. Most employees are also exposed on social media where their profiles can be used to predict or influence personal behaviour/reaction in an industrial context.

Based on this background, it would be appropriate to distinguish between four focus areas to investigate ICT vulnerability related to telework:

A. ICT vulnerabilities that can disrupt or create doubts about the security of the individual worker's remote access to one or more target systems or applications

B. ICT vulnerabilities related to telework where this is included in the type of interaction described above (as an HTO balance between primary and secondary work), and which may threaten the integrity of such interaction

C. ICT vulnerabilities related to the possibility that trends and complex industrial threat landscapes that emerge in other areas of society, such as hacking, prepared / orchestrated projections, commercial, financial and political impact, are also contagious and manifest in the industry's industrial ICT systems

D. ICT vulnerabilities related to industrial threat landscapes being linked to external ICT threat landscapes (e.g. through employees and companies being available on and profiled through social media)

Telework is affected by the IT/OT integration problem. Although, in principle, the remote access should go directly into the OT domain, the security on the way in will be influenced by the general ICT security and associated practices in external (IT) domains.

The combination of IT and OT is constantly challenging. It is considered that it is significantly more difficult to keep track of and monitor ICT security in industrial ICT systems. Technical and cultural differences provide a ripple effect that both creates vulnerability and restricts the use of common ICT security measures. For example, tools for intrusion detection are not used in the OT domain in the same way as IT, user rights management practices may be different, and industrial ICT systems generally stand out by being designed for high reliability and functional integrity, and greater degree of autonomy. Dependency on dedicated system vendors for OT maintenance and error correction can be significant, the boundaries between operational disruptions and security breaches can be unclear (and difficult to interpret from a more general IT perspective), and different practices and interpretations may even create a foundation for misunderstandings in these borderlands. While interest in "agile" system development on the general ICT side is also growing in the petroleum industry, such trends are met with (justified) scepticism in the OT domain, which confirms the gap in security approach between the two domains.

In the following, point A and B of ICT vulnerabilities highlighted above in particular are elaborated on.

(A) ICT vulnerabilities that can disrupt or create doubts about security of remote access

On the basis of the IT/OT problem understanding described above, it is interesting to understand how the perceived vulnerabilities appear to the industry and its expectations and experiences of telework, and whether the ICT security regimes actually support telework in a good way so that it safeguards safety and confidence in the basic teleworking situation.

In approaching this issue, we can also draw on the distinction of primary work vs. secondary work (articulation work) that we have discussed through the complexity perspective. That is, we can examine whether and to what extent both the telework and the underlying cyber security practices that create the necessary security are exercised under a primary work "recipe" or standards that are legitimized through policies or procedures, whether they also comprise "secondary" work, and whether the latter happens informally or "secretly". It will also be interesting to understand whether secondary practices also require articulation work between, for example, system owners, system suppliers, subcontractors and users.

(B) ICT vulnerabilities that could threaten the integrity of interaction and HTO balances

An important issue is how ICT-related vulnerability can affect telework-based collaboration as described under "Increased complexity in the form of (ICT-supported) interaction" above. Therefore, the area of interest ultimately points to forms of ICT security that contribute to safeguarding critical HTO balances, and we should be concerned about the potential impact of the balance between primary and secondary work, including articulation work. The questions that can be asked will be derived from (a selection of) the questions we defined above under the theme "Increased Complexity of Interaction", with orientation towards:

- whether we see any actual distinction/priority between vulnerability and protection of primary/secondary/articulation work, respectively;
- if we see that perspective-making/taking is a process that is valued and supported (to the extent that it involves shared information objects),
- whether "boundary objects" are adequately supported/protected/valued;
- whether ICT support contributes to "shared forgetfulness", possibly contributing to logging this,
- whether "hyper-reality" is explicitly supported/legitimized as part of primary work,
- whether information spirals are given "energy" by giving "fresh" data priority,
- whether the ICT security regimes are sensitive to changes in foreground/background; are there any "moving compromises" related to ICT security in new decision-making contexts; who is responsible for (common) ICT security under changing circumstances; who gets the breakthrough, final words if there is a level of protection disagreement?
- whether ICT security practices support an ecology of actors/species with different interests, and their interaction (or is it a standardized protection "for all"?)
- whether the trust aspect is prominent in the definition of security requirements

These issues are of such a nature that they will not immediately be recognized as relevant to ICT security in the traditional sense. First, it will be relatively demanding to map typical security categories such as confidentiality, integrity, accessibility, authenticity and non-repudiation to the information objects included in the interaction that correspond to the issues. In addition, there will be a limit to the extent and in what way technical mechanisms can replace the social/relational mechanisms that Hepsø (2006) points to as essential for trust and mutual commitment, e.g. which (other) persons a given person trust to the extent that this offsets self-doubt about the integrity of a critical information object. Although ICT security can safeguard a person's authenticity, this person's credibility and integrity in sociotechnical interaction with other in telework, must be otherwise supported. At some point, therefore, we will have to seek an "ICT security" that supports doubt rather than blind trust (e.g. to "news"), and which provides the user with tools to deal with this doubt through clarifying for example origin and history of information sources, and possibly suggest other sources and filtering of information in such a way that the user's knowledge process is supported in the right direction. There is a lot of unploughed land here.

Dilemma between organizational safety vs. ICT security

Organizational safety, including HTO interaction, has gained an ever-stronger place in the safety work in many industries, including the oil and gas sector. This includes a growing trend towards the recognition of the need for a good mix of "Safety-I" and "Safety-II", the latter often denoted "resilience".

As put by Hollnagel (2014), *the traditional view of safety, called Safety I, has consequently been defined by the absence of accidents and incidents, or as the 'freedom from unacceptable risk.' As a result, the focus of safety research and safety management has usually been on unsafe system operation rather than on safe operation. In contrast to the traditional view, resilience engineering maintains that 'things go wrong' and 'things go right' for the same basic reasons. This corresponds to a view of safety, called Safety-II, which defines safety as the ability to succeed under varying conditions. The understanding of everyday functioning is therefore a prerequisite for the understanding of the safety performance of an organization.*

Successful implementation of Safety-II, or resilience, thus rests on the conditions for secondary work also in the telework context.

One possible line of development is however that the premises for successful Safety-II are weakened through telework, because the actual actions of secondary work require local insight and proximity. The more subtle parts of this can become less tangible, and easily get lost in a "re-presented" hyper reality mainly focused on primary work. Safety-I can, paradoxically, again become the safe haven, at least for the actor that is rendered only the option of complying with ICT-secured "primary work". ICT security can "bind" the interaction, and "digital security" can thus be more biased towards supporting Safety-I alone, than what reality require in terms of safety thinking.

If this is to be avoided, also the cyber security approach per se must be founded on a recognition of digital complexity. This way, it is possible to conceive a "cyber resilience" that deals with cyber security threats and vulnerabilities in a manner that does not jeopardize the conditions for a successful implementation of "Safety-II" as an integral part of telework, and that also may convert this insight into to a "Security-II" that may be an important constituent of cyber resilience.

Conclusion

There is a need for a deeper understanding of how digital complexity affects remote work.

The discussion in this paper is anchored in a decade-old perspective that is still relevant.

It is apparent that for any concept of "cyber resilience" to be relevant, digital complexity must be appreciated, and the perspective of sociotechnical interaction must encompass some resemblance of the issues discussed here in terms of HTO balances. This applies not only for the telework case.

However, key issues need to be elaborated more, not at least in order to reflect contemporary trends related to industrial applications of "Big Data", machine learning and artificial intelligence.

Acknowledgement

The paper is based on selected excerpts from Bodsberg et al. (2018), which was financed by the Norwegian Petroleum Safety Authority.

The actual selection and its presentation in this paper is adapted to a broader project of theoretical advances on cyber resilience (TECNOCRACI), funded by the Norwegian Research Council, under contract no 303489.

References

Bochman, A. 2018. The End of Cybersecurity. Harvard Business Review

Bodsberg, L., T.O. Grøtan, M.G. Jaatun, T. Onshus and I. Wærø (2018), ICT Security – Remote work and HSE work (In Norwegian - " IKT-sikkerhet – Fjernarbeid og HMS "), SINTEF Report 2019:00361, Trondheim, Norway

Greenberg, A. 2019. Sandworm: a new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Doubleday

Grøtan, T.O. (2007). ”IKT som bidrag til robusthet i integrerte operasjoner – et skråblikk”. I Tinmannsvik, R.K. (red) Robust arbeidspraksis. Hvorfor skjer det ikke flere ulykker på sokkelen? Tapir, Trondheim

Grøtan, T.O. and E. Albrechtsen (2008), Risk analyses of Integrated Operations with respect to technological, human and organisational factors (In Norwegian – "Risikokartlegging og analyse av Integrerte Operasjoner (IO) med fokus på å synliggjøre kritiske MTO aspekter"), SINTEF report A7085, Trondheim, Norway

Grøtan, T.O., 2018. Building Cyber Resilience through a Discursive Approach to "Big Cyber" Threat Landscapes. ESREL 2018. June 2018, Trondheim, Norway

Hepsø, V., 2006. Intelligent energy in E&P: When are we going to address organizational robustness and collaboration as something else than a residual factor? Paper at the 2006 SPE (Society of Petroleum Engineers) Intelligent Energy Conference and Exhibition in Amsterdam, The Netherlands, 11-13 April 2006. See https://www.onepetro.org/conference-paper/SPE-100712-MS

Hollnagel, E. 2014. Safety-I and Safety-II. The Past and Future of Safety Management. CRC Press

Johannessen, S., 2017. Strategies, Leadership and Complexity in Crisis and Emergency Operations. Routledge Advances in Management and Business Studies

Kallinikos, J. 2006. Information out of information. On the self-referential dynamics of information growth. Information Technology & People, 19(1), 98-115

Kurtz, C.F., Snowden, D.J. 2003. The new dynamics of strategy: Sense-making in a complex and complicated world. IBM Systems Journal, Vol 42, No 3, pp 462-483

Milch, V. 2018. The influence of interorganizational complexity on safety: Safety challenges and opportunities in the petroleum industry. Doctoral Thesis at NTNU, Trondheim (2018:219)

Sørhaug, T. (2004). In Norwegian: Managementalitet og autoritetenes forvandling. Ledelse i en kunnskapsøkonomi. [Management and the transformation of authorities. Management in a Knowledge Economy]. Fagbokforlaget

Turner, B., 1978. Man-made disasters. Wykeham Publications, London.

Weick, K.E., 1998. Foresights of Failure: An Appreciation of Barry Turner. Journal of Contingencies and Crisis Management. Volume 6, Number 2, June 1998, pp 72-75Alvesson, M., &

Zuboff, S. 2019. The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power. Profile Books