Title

Cyber-conformity and safety: the groupthink dilemma

Author
Fred Størseth

Biographical notes
Fred Størseth holds a Doctoral degree in Psychology (2005) and background as Senior Research Scientist on Safety. He currently holds a position as Post-doctoral researcher. His research interests include: cyberpsychology, organisational safety, resilience engineering, safety management and societal safety.

Contact info
Email: fred.storseth@ntnu.no
Email: fred.storseth@gmail.com
Mobile: +47 458 64 330

Postal address
Norwegian University of Science and Technology, NTNU
Department of Psychology
NO-7491 Trondheim
Norway

Reference to this paper
This document is the *accepted manuscript*. The correct reference to the paper is: Størseth, F. (2017) 'Cyber-conformity and safety: the groupthink dilemma', Int. J. Decision Sciences, Risk and Management, Vol. 7, No. 4, pp. 316-331.

Abstract

The 'capable group' is part of the ethos in resilience-based safety management. Group ideas draw upon psychology. But, what if the psychological blueprints no longer apply? My thesis is that we are changed by c*yber-conformity:* A trait-like propensity grooved into our psychology as we immerse ourselves in the ever-present digital social spheres for attention, confirmation and approval of 'the others'. What if cyber-conformity renders aspects of group psychology obsolete? In applied safety, decision-making accentuates group dynamics under pressure. Is the group still 'capable'? The aim is to explore how cyber-conformity spills into group dynamics, and in turn plays out in decision-making. With groupthink as analytical approach, the paper identifies the 'groupthink dilemma', i.e. although the conventional 'ingroup' loses meaning, the dangers of groupthink is as strong as ever. It is discussed how group-based decisions tinted by cyber-conformity forms the potential of 'long-distance groupthink' and funnel-vision decision-making.

Key words: Conformity, decision-making, group dynamics, groupthink, internet, information technology, psychology, safety management, safety method, social media.

Introduction

The 'capable group' is part of the ethos in resilience-based safety management. Group performance is vital when conceptions of resilience are pushed into operative detail. By building on ideas of group functioning, resilience draw upon psychology. However, this connection is typically left unspoken. Social psychological group principles are silently referred to, serving to validate the intended group resolve. But, what if the psychological blueprints no longer apply? Put differently: What if the psychological principles that resilience silently rests upon no longer holds?

This paper pursues this possibility by exploring the *Cyber-Conformity Thesis*. Cyber-conformity is defined as an exaggerated social sensitivity specifically linked to our constant orientation towards 'the others' in digital social spheres. What if cyber-conformity corrodes group identity, focus and loyalty to a point where the intended group function is lost? The underlying thesis being that the digital omnipresence in our lives imposes deep changes in our psychology.

If cyber-conformity renders aspects of group psychology obsolete this denotes a need for resilience-based safety (and any approach based on human performance), to explicitly consider the psychological underpinnings that are used to validate the group dynamics that their methods are based on. In applied safety approaches, *decision-making* is of particular interest as it accentuates group dynamics and performance under pressure.

By calling attention to group-based decision-making the issue of '*groupthink*' springs forward. Groupthink is a well-known byproduct of group decisions; a consensus-seeking *conformity* so strong that it restricts and destroys the decision process (Janis, 1971). As groupthink theory is built around the detrimental potential of conformity, this connects with

the key premise of this paper (i.e. the potential of cyber-conformity). Groupthink theory will thus be used as analytical vantage point throughout this discussion.

Problem specifications

The aim is to explore how cyber-conformity spills into group dynamics, and in turn plays out as groupthink in decision-making. The reference point for this discussion will be resilience-based safety – as representative of group-based safety management. Nevertheless, it should be recognized that the discussion transfers to any organisational or management setting. Ideas pertaining to teamwork and group performance pervade organisational philosophies and management approaches. As noted by Salas et al. (2015), teamwork has become the backbone of organisational life.

Please note that the 'group' concept is here used as the equivalent to 'team'. It is recognized that a more stringent distinction can be applied, e.g. that 'team' denotes a group with goal directedness, while 'group' may merely denote a category of participants (see e.g. King, 2002 for an overview of the literature on team versus group).

Methodological position

The methodological position of this paper is inspired by the theory is method approach (Størseth and Grøtan, 2011), advocating active application of theory, in order to systematically pursue and explore theoretical ideas and conjectures. The idea is to engage in theoretical groundwork, to develop and pursue ideas, and intentionally take conjectural steps beyond mere description of the status quo.

Paper format

The paper is written as a theoretical discussion that builds and defends the cyber-conformity thesis by reference to ideas of resilience-based safety, groupthink and decision-

making. The work is written as a classical academic thesis, where theoretical elements and principles are presented and discussed throughout the article. Each key discussion segment is summarized by formulating a proposition that captures the theoretical point being made.

Paper structure

The thesis is built as follows: First, principles of resilience-based safety are described to create a *case example* (reference point) for the discussion on cyber-conformity and group-based decision-making. Second, the cyber-conformity thesis is presented. Third, the proposition that this conformity defuses foundational concepts of group psychology is presented and discussed. Fourth, groupthink theory is used as framework to explore new patterns of group dynamics in the light of cyber-conformity. Finally, implications of the cyber-conformity thesis are discussed.

Resilience-based safety

Resilience Engineering (e.g. Hollnagel and Woods, 2006) continues to gain momentum in all things safety. Resilience-based ideas are increasingly considered viable complements to traditional safety management. See Rosness et al. (2010) for a comparative analysis of Resilience Engineering in relation to other safety management perspectives.

Hollnagel defines resilience as: '… an expression of how people, alone or together, cope with everyday situations – large and small – by adjusting their performance to the conditions. An organisation's performance is resilient if it can function as required under expected and unexpected conditions alike (changes/disturbances/opportunities)' (Hollnagel, 2018, page 14-15).

The definition shows how resilience is about performance and functioning based on coping and adjusting. A core feature in resilience is in other words *adaption*. The performance

of a system (organisation) must be capable of adjusting and adapting the situation. Put differently, the organisation copes by adjusting (Hollnagel, 2012). From a psychological point of view this draws attention to human performance: Who will do the coping – and how?

In Resilience Engineering, attention is turned towards why 'things' work; i.e. what makes the organisation capable of performing adequately. According to Hollnagel, resilience is 'a characterization of certain kinds of performance …' (Hollnagel, 2018, page 26). The approach to understand the performance of a system (organisation) is to consider the resilient *potentials for performance*.

Resilient potentials

Resilience Engineering proposes four potentials for resilient performance. These are the potential to (1) respond (knowing what to do), (2) monitor (knowing what to look for), (3) learn (knowing what has happened / learn from experience) and (4) anticipate (knowing what to expect). These resilient potentials are generically defined by intention, because they reflect possible capabilities for most (if not all) organisations (Hollnagel, 2018).

The analytical attention in resilience gravitates towards organisational performance (ibid). However, in applied safety management approaches – resilience is operationalized and explored along several organisational levels: the individual, the team, and the organisation (Bergström, van Winsen and Henriqson, 2015).

In fact, teamwork and team performance are key concepts in resilience in relation to managing and responding to emergency and danger (see Bergström et al. (ibid) for a literature review on the rationale for resilience. Simplified, it can be argued that when resilient potentials (as described above) are operationalized and prepared for practical use – the team (group) performance is an integral part of operative safety management. Thus, in operative

resilience-based safety management, the capable group (team) is a designated unit of resolve. A unit appointed to identify, respond to, and handle danger and emergency. To realize these demands, team training is a pronounced part of resilience-based safety management (see e.g. Grøtan et al., 2016). It should be mentioned that ideas pertaining to resilience and teamwork are being advocated as important for any business and organisational area – and not only in high-risk domains (Alliger et al., 2015).

The intention here was not a comprehensive rendition of resilience-based safety theory. The point was to create a *case example* of the resilient performance potentials and how teamwork and group performance are integral when resilience is operationalized and pushed towards the operative.

By suggesting how teamwork is integral in the operative resilience scope, I will argue that this supports the very premise of this paper: That resilience-based safety is pervaded by a group ethos; and that this in turn represents a 'silent reference' and application of group-based psychological concepts. With this case example as thematic background, the discussion can be initiated by considering the following possibility: What if the blueprint no longer holds? What if the group-psychological principles that resilience silently rests upon no longer holds? This will here be explored by the cyber-conformity thesis.

Cyber-conformity

Eagerly we log on to social networks, to immerse ourselves in digital torrents of attention, confirmation and approval of 'the others'. What have become of us? It has been suggested that the digital omnipresence in our life imposes a deep change in our psychology; a change towards conformity and compliance (Størseth, 2013). This variation of conformity appears as a trait-like tendency, recognized and expressed as 'exaggerated social sensitivity'. This hyper-social propensity is grooved into our psychology by the relentless logic of (1)

massive exposure of digital social tools; and (2) the way that these tools tap into human needs of being seen, heard and recognized (Størseth, 2013). This conformity will in this paper be referred to as *'cyber-conformity'*. Thus, I initiate my thesis by arguing that a cyber-induced conformity leaks into our psychology and changes us as human beings.

To understand this 'digital surrender' it is significant to consider Zuboff's thesis concerning the ever-expanding computer-mediation, and how our entire existence is redefined and digitally reborn. The world is so computer-mediated that even the idea of an alternative is challenging. The inevitability is overwhelming (Zuboff, 2015).

This is comparable to Foley's 'anonymous authority', a power variation with its most powerful feature being that it appears self-evident to a point of being impossible to oppose and argue against. Accordingly, the implication is that the way we live now reaches the standing of 'natural law' (Foley, 2010). We are at a point where 'social production' (Benkler, 2006, in Zuboff, 2015) via social media are considered mandatory for social participation.

In Størseth (2013) it is argued that this 'inescapable' digital reality shows itself as a twin pull of 'self-reduction' and narcissism.

Self-reduction and narcissism

Based on Lanier's *'You are not a gadget'* (Lanier, 2011), it is in Størseth (2013) argued that we occupy ourselves with 'self-reduction'. We engage, rethink and reduce ourselves. With mindless eager we obey to the dictates of the digital design. We are debasing ourselves by organizing and defining ourselves downward to fit digital design solutions (Lanier, 2011). In Størseth (2013) this is described as *'self-reduction'* and are considered as connected to, and accompanied by 'narcissistic projects' of ever increasing proportions.

In Størseth (2013) the nature of these narcissistic efforts are described by reference to Alvesson's *'The Triumph of Emptiness'* (Alvesson, 2011). Alvesson emphasizes the widespread and heavy investment in portraying 'correct' and flattering images of ourselves. This erratic and narcissistic image management has become equal to construction of identity, if not personality (ibid). In Størseth (2013) it is advocated that a normal psychology saturated with narcissism resonates well with the extent of enthusiasm and obsessive self-display that can be observed in the digital spheres. On this rationale, I propose that:

> Proposition 1: Our engagements in the digital social spheres are infused by self-reduction and narcissism.

The twin pull of self-reduction and narcissism interplays with what is offered in the digital social spheres (social media). This interchange and interaction between fundamental human needs and digital tools produces an '*exaggerated social sensitivity*': A hyper-alertness directed to 'the others' out there in the digital, a constant hunt for approval, acceptance and acknowledgement (Størseth, 2013).

The sheer extent and pervasiveness of computer-mediation and digital living creates a silent consolidation of the state of 'exaggerated social sensitivity' towards a more stable and trait-like cyber-conformity.

As cyber-conformity spills into and changes our psychology, this may render aspects of group psychology obsolete. In other words, established psychological concepts for explaining and interpreting group dynamics may no longer apply. For resilience-based safety that leans heavy on group performance, this denotes an urgent need to reconsider the underpinnings of group dynamics. To initiate this, I advocate that:

Proposition 2: The potential of cyber-conformity creates a need to revisit foundational ideas of group psychology.

A critical concern in this paper is how cyber-conformity may impact safety (by reference to resilience-based safety management). It is theorized that cyber-conformity may change the 'formal logics' of group dynamics – and that this in turn may affect group performance (like decision-making). The cyber-conformity – safety hypothesis is illustrated in Figure 1.

Figure 1: The cyber-conformity – safety hypothesis.

Group psychology revisited

If cyber-conformity involves incessant vigilance towards 'the others' outside, how will this affect the group inside? With ceaseless distraction and interaction with the outside, what is left of the ingroup? Pursuing these questions, an option is to 'pressure test' psychological conceptions pertaining to: *'Group framing'* and *'Group template'*. What is the 'integrity' of these group ideas in the light of cyber-conformity?

Group framing

A defined group has a sense of borders or 'framing' that builds 'group demarcation' and unity. A group can be 'framed' by e.g. defined tasks, objectives, functions and so on. The sum of these defining features creates a sense of distinction, or border that 'frames' the group unit. This group framing helps the group members to direct focus and attention towards each other, to interact, build trust and collaborate.

By the premise of cyber-conformity, it can be argued that these group demarcation lines are 'perforated' by incessant efforts to seek 'others' for attention, confirmation and acceptance. This hunt for approval constantly disrupts the group borders by involving 'others' from the ever-present digital audience. Locked into a perpetual mode of image management, the presence of a 'digital target audience' is a constant in the minds of digitally addicted crowd pleasers. The continuous hunt for attention and confirmation threaten to destroy the solidity of the group framing. The defining group lines are punctuated by endless 'flickers of attention' desperately seeking approval. This scattered attention and restless vigilance towards the digital audience is a corroding force that may disintegrate group identity, focus and loyalty to a point where the intended group function is lost.

Group template

Although group configurations vary in terms of functions and goals, some element of collaboration is typically part of the validation in resilience-based safety management settings. The group is formed on the presumption that the group's defined purpose is realized by some collective effort of its members. Collaboration is thus a central group validating idea. Intragroup loyalty and unity are also defining principles. A sense of allegiance builds focus and motivation towards a collective problem solving. Such ideas (collaboration, unity,

loyalty) are part of the group code, or 'group template', i.e. core conceptions that defines and validates the group.

With cyber-conformity, it is as if the group template has no solid ground. It transforms into a 'stage' to display sociability and 'correctness' to the digital audience outside of the group unit. The group as a defined space for purpose and determination may thus be lost to a fervent adaptation towards consensus and harmony. The search for harmonious consensus becomes 'a leveler' serving to defuse both ambition and ability to seek outside the pleasant state of socially approved averages. Based on the above, I will propose that:

> Proposition 3: Cyber-conformity creates a restless and incessant need for social acceptance so strong that it changes the 'blueprints' of group functioning.

If this (Proposition 3) is the case, it is imperative for both psychology and group-based safety management to acknowledge this, and to expand theoretical groundwork pertaining to group performance.

In operative safety settings, *decision-making* under pressure is a challenge that accentuates group performance. In the light of cyber-conformity, the question that should be asked is this: *Is the group still 'capable'?*

To examine this question I will focus on *groupthink* (e.g. Janis, 1971); a well-known side effect in group decision-making. Groupthink theory combines internal (group) dynamics with external circumstances. Based on this, I propose that:

> Proposition 4: Groupthink can be used as analytical framework to explore and extrapolate a group psychology tinted by cyber-conformity.

Groupthink

The original groupthink theory was developed by research psychologist Irving L. Janis. He presented the outlines of the theory in 1971, and described groupthink as a decision mode so driven by consensus-seeking and harmony that it 'tends to override realistic appraisal of alternative courses of action' (Janis, 1971, page 84). Groupthink and its potential contribution to unfortunate and disastrous decision-making have become well-known. Outside psychology, groupthink is addressed in fields like business, political science, communication and management training (Esser, 1998).

It is interesting to note how Janis contextualizes groupthink by drawing a parallel to Orwell's '1984' (Orwell, 1949). According to Janis 'groupthink is a term of the same order as the words in the newspeak vocabulary George Orwell used in his dismaying world of 1984' (Janis, 1971, page 84). With this reference, 'groupthink takes on an invidious connotation' (ibid). Janis emphasize that this undertone of unpleasantness is very much intended, as the pressures of groupthink involves deterioration in mental efficiency, reality testing and moral judgments (ibid). The classic specification of the groupthink model is presented below.

Classic groupthink

The groupthink theory specifies how 'extreme concurrence-seeking' in decision-making groups contributes to defective judgments and outcomes (Janis, 1982, in Turner, Pratkanis and Struckman, 2014). Groupthink denotes a decision process of intragroup conformity pressure (ibid).

The classic model suggest how groupthink is most likely to occur by the contribution of a set of *Antecedent Conditions*: [The group is] highly cohesive, insulated from experts, perform limited search and appraisal of information, operate under directive leadership, and

experience conditions of high stress with low self-esteem and little hope of finding a better solution to a pressing problem than that favoured by the leader or influential members. The presence of these precursors predicts a mode of extreme *consensus-seeking*. This drive towards harmony is hypothesized to lead to two undesirable symptom categories: (1) *Groupthink symptoms* and (2) *Defective decision-making symptoms*.

Groupthink symptoms includes: Illusion of invulnerability, collective rationalization, stereotypes of outgroups, self-censorship, mindguards (i.e. self-appointed 'protectors' of the group complacency; see Janis, 1971), and belief in the inherent morality of the group. In turn, this leads to the *Defective decision-making symptoms*: Incomplete survey of alternatives and objectives, poor information search, failure to appraise the risks of the preferred solution, and selective information-processing. Ultimately, the predicted outcome is h*ighly defective decision-making* (Turner et al., 2014, page 224). The classic groupthink model of antecedents and consequences is illustrated in Figure 2.

Figure 2: The classic groupthink model (e.g. Janis, 1982).

Can the classic groupthink model be used to expand group-theoretical grounds in a way that acknowledges cyber-conformity?

Figure 2 shows how consensus-seeking is predicted to lead to two sets of unfortunate symptoms (groupthink and defective decision-making). These symptoms combined are

hypothesized to lead to highly defective decision-making. As cyber-conformity is the tendency of exaggerated *social* sensitivity, it connects thematically with the concurrence-seeking tendency in groupthink. On this premise, I propose that:

> Proposition 5: The classic groupthink symptoms are analytical focus points to explore decision-making in the light of cyber-conformity.

The groupthink dilemma

The symptom classes of the classic groupthink model denote areas of particular interest in a decision-making process impacted by cyber-conformity. By substituting concurrence-seeking with cyber-conformity, groupthink becomes an approach to study how cyber-conformity potentially leads to a *'funnel vision'* decision-mode, a narrowing, and unfortunate focus on maintaining agreement and harmony.

At this point however, a significant dilemma springs forward: Groupthink is a decision-process of *intragroup* conformity pressure (Janis, 1971). How does this translate into cyber-conformity, a tendency that arguably has changed the 'blueprints of group functioning' to a state where the intragroup focus is lost? This will here be referred to as '*The Groupthink Dilemma'* and is elaborated in the following.

With cyber-conformity, the antecedent conditions of the classic groupthink model (Fig.2) lose explanatory power. As cyber-conformity turns group members away from its 'actual' group and towards 'the others' out there in the digital social spheres – this challenges ideas pertaining to ingroup influence. And, if the conventional ingroup loses meaning – the antecedents of the classic groupthink model may not be suitable to explain groupthink.

The crux of the matter is this: classic groupthink is an important 'map' to show the dangers of 'funnel-vision' decision-making in groups. But, if the 'ingroup' blueprint has changed by cyber-conformity – how can 'funnel-vision' be identified and mitigated?

Although the dangers of groupthink are as present as ever – the ingroup cohesion is 'gone'. A key to challenge this dilemma may be to put emphasis to the core characteristic of cyber-conformity: the exaggerated *social* sensitivity. The social nature of cyber-conformity spurs attention towards a particular variation of groupthink theory that explains groupthink as a way to protect and maintain *social* identity. This is the *Social Identity Maintenance (SIM) model of groupthink* (Turner, Pratkanis, Probasco and Leve, 1992; Turner and Pratkanis, 1998, in Turner et al., 2014).

The SIM model advocates that groupthink may occur as a result of a drive to maintain and protect a positive social identity. The emphasis on social identity makes the SIM model thematically interesting in relation to cyber-conformity (as exaggerated social sensitivity). Based on this connection, I will propose that:

> Proposition 6: Social identity protection suggests how cyber-conformity may create '*long distance groupthink'* initiated 'out there' in the digital social spheres that ricochets back and obstructs resolve in the '*actual ingroup'* (e.g. resilience-based safety team).

The following section introduces the SIM model and explores how it may be used to face 'The Groupthink Dilemma', i.e. to identify and understand long distance groupthink induced by cyber-conformity.

Long distance groupthink

The SIM model suggest how a collective threat may shift the group focus into an 'identity protection mode' that is detrimental for group decisions. See Figure 3.

Figure 3: Social identity maintenance model of groupthink (e.g. Turner et al., 1992).

The SIM model advocates that 'groupthink occurs when members attempt to maintain a shared positive image of the group' (Turner et al., 2014, page 230). This prediction is based on two assumptions. First, it is assumed that group members must develop a *positive group image*. Second, this very image must be challenged or questioned by some collective threat. Both of these are held to be essential conditions for developing groupthink as (social) identity protection.

Group self-categorization. The first condition in the SIM model is that group members must consider and classify themselves as a group, as opposed to individuals drawn together (Turner et al., 2014). How may this apply in a state of cyber-conformity? A vital difference is that cyber-conformity changes the direction of group identification. Established conceptions delineate an inward directed path of group identification (towards the ingroup). However, with cyber-conformity, focus shifts 180 degrees – and turns outward. By this reasoning, I will argue that:

> Proposition 7: With cyber-conformity, the 'self-categorization' precondition still applies, but the focus is directed away from the actual ingroup – and towards the ever-present 'others' in the digital social spheres.

Another way to describe this is that 'the others' in the ever-present digital takes on a role as a vicarious *'digital ingroup'*; a group that incessantly instils its members with a sense of social identity – and control. In line with the SIM precondition that they (participants) must perceive the group as having a social identity, this translates to the state of cyber-conformity. The radical difference is who acts as functioning intragroup.

Continuing with Turner et al.'s (2014) specification of the SIM model, it is assumed that group 'self-categorization' is linked to three consequences: (1) positive group image, (2) identity protection and (3) defective decision-making.

Positive group image. Categorization leads to a tendency of creating and protecting a 'positive group image'. For instance by the group seeking to form a positive ingroup distinction; and exhibiting motivational bias for positive collective self-esteem. Another process may involve the reinforcing of similarities between individuals and other group members. This makes the group identity attractive, and it creates a basis for cohesion (Turner et al., 2014). These are conventional ingroup efforts to form image and a sense of commune.

With cyber-conformity, the potential is however that attention and effort gravitates towards the digital ingroup to a point of overshadowing the actual ingroup. And so, by a similar logic as suggested regarding self-categorization (Proposition 7), I propose that:

> Proposition 8: In the light of cyber-conformity, ingroup consolidation shifts towards the digital social spheres to the extent of potentially obstructing group focus and resolve of the actual ingroup (e.g. resilience-based safety team).

In addition to the Positive Group Image effort, the SIM model specifies the presence of a collective threat to the group image:

Collective threat. A form of collective threat 'attacking' the positive group image is a second condition in the SIM model. Threat is defined as the 'potential of loss to the group' (Turner et al., 2014 page 232). It is emphasized that this threat is collective by nature, and that it must 'question or attack' (ibid) the group identity.

With cyber-conformity, the threat in a collective sense loses its meaning. That is, the unified focus of the conventional ingroup is shattered by how each member individually directs attention away from the 'actual' group in a constant hyper-sensitive mode directed towards the digital social. Thus, cyber-conformity can be assumed to dissolve the unified and shared response to a threat (perceived as 'attacking' the ingroup).

If a threat appears in a decision-process tinted by cyber-conformity, it is now a type of fragmented and individualized set of responses to this threat. These individualized responses can be thought of as individualistic trigger effects that add up, reaches a threshold effect and – by this dissolves the focus of the 'actual' group. Members are now too busy maintaining their image and status in the digital ingroup. On this rationale, I propose that:

> Proposition 9: With cyber-conformity, the threat response shifts into individual attempts to preserve their own status in the digital ingroup.

Although the response no longer comes from a unified actual ingroup, the sum of the individualized protection efforts may reach a threshold state where focus on the 'actual' group is lost to a restless state of ensuring each members' own identity within the digital ingroup. Thus, cyber-conformity creates a connection between the digital ingroup and the 'actual' operative group. This proposes a possible path of influence between the digital ingroup and

the actual group; a passage that allows for long distance groupthink effect. Having justified the possibility of a long distance groupthink, attention is returned to the SIM model. According to the model, identity threats triggers identity protection.

Identity protection. A threat creates a dissonance that activates groupthink processes in order to regain control of the social identity. Faced with a collective identity threat, the tendency is to focus on cues that maintain the shared positive group image. This may be detrimental for the group functioning (Turner et al., 2014).

Put differently, focus may narrow down so that image protection becomes the dominant task. This is similar to what I named *'funnel vision'* in relation to the classic groupthink model (Janis, 1971). In the SIM model however, the tapering or contraction of focus is specifically linked up to the attempt to protect social identity. When cyber-conformity enters the equation, the logic is no longer to protect the collective identity of the 'actual' ingroup. Rather, I advocate that:

> Proposition 10: With cyber-conformity, the identity threat is individualized and personal. Individual members of the 'actual' group are predominantly focused on how the threat affects their own position and standing in the digital ingroup.

Group protection is thus the sum of individual efforts to comply with the digital ingroup. The digital ingroup is protected by how individuals strive to protect their own position and image – to ensure that it is kept within the accepted frame of the digital ingroup. In this way, cyber-conformity establishes a new ingroup focus, and with it a new logic in terms of how to protect its identity and status. Regardless of this shift in focus however, the result is still the same: Groupthink – and with it – the potential of defective decision-making follows.

Defective decision-making. According to Turner et al., cohesion alone may *positively* facilitate group decision performance and group goals. However, when a threat to the collective identity arises, this may jolt the group focus into identity protection mode. It is the interaction of cohesion and threat that may affect group decisions negatively. This narrowing of attention 'detracts from the decision-making process to such an extent that performance is impaired' (Turner et al., 2014, page 233).

As have been emphasized in this this paper, cyber-conformity substitutes conventional ingroup cohesion with a digital ingroup unity 'out there'. On this premise, it is this digital unity that interacts with a threat. To circle in on the threat, it is important to note that the thematic backdrop in this paper is decision-making in a safety or security context (e.g. as performed by a resilience-based safety team). That is, decisions under pressure and uncertainty; decisions that may produce massive and irretrievable outcomes. In this way, it can be said that the decision becomes the threat.

Each individual member of the actual ingroup may perceive this threat (i.e. critical decisions with high-risk potential) as personal and private. But with cyber-conformity their sense of 'private', their core sense of person is tightly connected to their identity and image management in the digital ingroup. By this rationale, a perceived personal attack on identity and image becomes a threat to the digital ingroup. Based on this, I propose that:

> Proposition 11: With cyber-conformity, the sense of unity with digital ingroups combined with the threat of critical decisions may trigger identity protection that entails long distance groupthink and funnel vision decision-making.

With proposition 11, the cyber-conformity thesis is completed. Attention is now directed towards potential repercussions.

Discussion

In true spirit of our times, cyber-conformity distracts attention and misplaces group focus to 'somewhere else'. To conjure up an image: The 'actual ingroup' now consists of people standing in a circle, their faces turned outward – towards 'the others' – in their respective 'digital ingroups'. In a restless and hyper-vigilant state their scattered focus is forever tuned into the attempt to seek attention, confirmation and validation. A sense of unity in the 'actual ingroup' pales by a shattered ability to stay focused on the task at hand.

The fundamental proposition permeating this paper is that cyber-conformity changes us as human beings. This has been examined by building a thesis that shows how the group psychological blue-print may have changed. As core premises for group functioning has transformed, so has the patterns and dynamics involved in group based decision-making.

With groupthink theory as analytical approach, the paper identifies a new group logic that should be considered in operative group decision-settings. As the ingroup focus has paled, a new 'long distance groupthink' is recognized as a conformity threat that may lead to defective and disastrous decisions. The drive towards harmony is the same as in the classic groupthink model, but the ingroup is digital and ever-present; with a funnel vision effect that works long distance.

Implications

Although the thesis in this paper has been categorical in tone and demeanour, this should be recognized as 'academic technique' with the purpose of distilling and accentuating the problem at hand. The changes induced by cyber-conformity will in reality be more subtle and moderate. A more temperate level of changes is however not an argument to dismiss the thesis. In fact, it is a case for the opposite: The subtleness of these changes, the elusiveness of

a silent movement towards conformity brings urgency to the thesis. The changes may be small and work in a slow pace; but, they may already 'have coloured the waters' of group dynamics. These changes have repercussions for both psychology and safety.

Safety. The cyber-conformity thesis underscore that it is no longer sufficient to silently refer to 'some' group psychological principle to justify the performance of a designated safety team. It is no longer sufficient to merely specify training principles and skills to operate in complex decision contexts. The potential of cyber-conformity emphasize the need to pursue the specifics of group functioning.

For resilience-based safety (and any safety management approach based on human performance), the cyber-conformity thesis underscores the importance of going into detail and start working with the specifics of psychological principles (e.g. group-based decision-making in the light of cyber-conformity). It is time for safety management to elaborate on its psychological underpinnings, to go stringently into assumptions concerning human dynamics and performance. As the system- and organizing scope of safety methods has increased – so must the scope of human dynamics increase and be brought up to pace.

The cyber-conformity potential specifically proposes developing safety methods able to identify and capture new patterns of group dynamics and decision-making (e.g. 'long distance groupthink').

Psychology. The cyber-conformity thesis advocates a change in us as human beings. If so, psychology as a discipline must recognize it and develop conceptions to study it. To exaggerate, cyber-conformity appears to have left the 'formal logics' of group psychology outdated. That is, established group conceptions of *collaboration* and *loyalty* ('group template'), *group borders* and *focus* ('group framing') seems faded. In fact, the *'ingroup'* as

we know it may have transformed into a 'digital ingroup' out there in the digital ever-presence.

Although the 'formal logics' of group psychology have changed, the unfortunate potential of *groupthink* is still recognizable. However, with cyber-conformity, its behavioural pattern transforms into something else: Long distance groupthink. The challenge for psychology is now to pursue the possibility of a new type of group dynamics that is connected to our cyber-infused forms of existence.

Here, psychological research efforts should recognize the opportunity to collaborate with developments in applied safety management settings. By starting in an applied explorative mode, group psychology may develop concepts by 'reverse engineering'; i.e. by beginning in the applied and operative – studying, theorizing and observing – and then bring this into basic research theory development.

In turn, these basic research expansions are brought back into the operative and applied safety settings. This involves hermeneutical oscillation between development of group psychological concepts and principles (basic research) and testing and establishing new hypotheses (applied research). As group psychology develops theory that reaches into cyber-life, this may expand the group conception repertoire as used in safety management.

Conclusions

The cyber-conformity thesis demonstrate the value of *problematizing* group functioning; and that it is time to explore new group dynamics and patterns of influence. This exploration may serve to identify ways to mitigate the corroding potential of long distance groupthink, funnel vision decision making – and other unfortunate group dynamics.

Safety management typically takes place within complex contexts of collaboration and interaction across a wide range of actors, organisations and interests. On this background, the prospect of cyber-conformity and its impact on group decisions underscores the need to draw new maps of group dynamics, and to systematically include conformity as a potential 'disturbance' moderating the capable group ethos.

References

Alliger, G.M., Cerasoli, C.P., Tannenbaum, S.I. and Vessey, W.B. (2015) Team resilience: How teams flourish under pressure, *Organizational Dynamics*, Vol. 44, pp. 176-184.

Alvesson, M. (2011) *Tomhetens Triumf* [The Triumph of Emptiness]. Atlas publishing company, Stockholm.

Benkler, Y. (2006) *The Wealth of Networks: How social production transforms markets and freedom*. Yale University Press, New Haven.

Bergström, J., van Winsen, R., & Henriqson, E. (2015) On the rationale of resilience in the domain of safety: A literature review, *Reliability Engineering & System Safety*, Vol. 141, pp. 131-141. doi:10.1016/j.ress.2015.03.008.

Esser, J. K. (1998) Alive and Well after 25 Years: A Review of Groupthink Research, *Organizational Behavior and Human Decision Processes*, Vol. 73, pp. 116-141.

Foley, M. (2010). The Age of Absurdity. Why Modern Life Makes it Hard to be Happy. Simon & Schuster, London.

Grøtan, T.O., Van der Vorm, J., Zuiderwijk, D., Wærø, I., Macchi, L., Evjemo, T.E., Veldhuis, G. (2016) *Guidelines for the preparatory work needed to implement a TORC (Training for Operational Resilience Capabilities) training program*, SINTEF report A27931, ISBN: 978-82-14-06184-0.

Hollnagel, E. (2012) Coping with complexity: past, present and future, *Cog Tech Work*, Vol. 14, pp. 199-205, DOI 10.1007/s10111-011-0202-7.

Hollnagel, E. (2018) *Safety-II in Practice - Developing the Resilience Potentials*; Routledge, New York.

Hollnagel, E., Woods, D. (2006) Epilogue: Resilience Engineering Precepts. In *Resilience Engineering – Concepts and Precepts*, edited by E. Hollnagel, D.D. Woods, N. Leveson, pp. 347-358. Ashgate, Aldershot.

Janis, I. L. (1971) Groupthink, (Reprint from) *Psychology Today Magazine*, Ziff-Davis Publishing Company, pp. 84-90.

Janis, I. L. (1982) *Groupthink: Psychological studies of policy decisions and fiascos* (2nd ed.). Houghton Mifflin, Boston.

King III, G. (2002) Crisis Management & Team Effectiveness: A Closer Examination, *Journal of Business Ethics*, Vol. 41, pp. 235-249.

Lanier, J. (2011) *You are not a gadget*. Penguin Books, London.

Orwell, G. (1949) *Nineteen Eighty-Four – a novel*, Secker & Warburg, London.

Rosness, R., Grøtan, T.O., Guttormsen, G., Herrera, I., Steiro, T., Størseth, F., Tinmannsvik, R.K., Wærø, I. (2010) *Organisational Accidents and Resilient Organisations: Six Perspectives. Revision 2*, SINTEF report (ISBN 9788214050561).

Salas, E., Benishek, L., Coultas, C., Dietz, A. Grossman, R., Lazzara, E., Ogleby, J. (2015). *Team Training Essentials – A Research-Based Guide*, Routledge, Taylor & Francis Group, New York.

Størseth, F. (2013) Digital culture conformity: contours of a 'new psychology' and its impact on safety. PSAM 2013, Tokyo, Japan, 14-18 April 2013.

Størseth, F., Grøtan, T.O. (2012) Safety theoretical issues: scientific please, but keep it brief. In: C. Bérenguer, A. Grall & C. Guedes Soares (eds.) 2012. *Advances in Safety, Reliability and Risk Management*, CRC Press, Taylor & Francis Group, London, ISBN: 978-0-415-68379-1.

Turner, M. E. and Pratkanis, A. R. (1998) A Social Identity Maintenance Model of Groupthink, *Organizational Behavior and Human Processes*, Vol. 73, pp. 210-235.

Turner, M. E., Pratkanis, A. and Struckman, C. A. (2014) Groupthink as Social Identity Maintenance, in Anthony R. Pratkanis (editor): *The Science of Social Influence – Advances and Future Progress*, edited by Anthony R. Pratkanis, pp. 223-246, Psychology Press, New York.

Turner, M. E., Pratkanis, A. R., Probasco, P. and Leve, C. (1992) Threat, cohesion, and group effectiveness: Testing a social identity maintenance perspective on groupthink, *Journal of Personality and Social Psychology*, Vol. 63, pp. 781-796.

Zuboff, S. (2015) Big other: surveillance capitalism and the prospects of an information civilization, *Journal of Information Technology* 30: 75-89.