Distrust: Not only in secret service organizations

Sabina Siebert and Barbara Czarniawska

Abstract

In this article we discuss the issue of distrust in the most extreme example of distrustful organizations: secret service organizations. Distrust may be a basic organizing principle in such organizations, but how is it produced and maintained? Inspired by Actor–Network Theory, we analyzed the devices, codes, rules, and procedures used in secret service organizations, and then asked if these devices, codes, rules, and procedures differ from those used in *ordinary* organizations. Based on our analysis, we make two contributions. Firstly, we draw researchers' attention to distrust that is intentionally built and maintained rather than distrust that is accidental and indicative of faulty management. Secondly, we identify the material manifestations of distrust. We argue that in future studies of trust and distrust in organizations, it will be necessary to focus on the technologies, physical objects, and quasi-objects. These, together with discourses, guarantee the stability of connections among organizational actions.

Keywords: Actor–Network Theory, distrust, objects and quasi-objects, secret service organizations, trust.

Our study stands in contrast to myriads of studies on trust in organizations that are based on the assumption that trust is necessary for the functioning of most, if not all, organizations (see e.g., Luhmann, 1979; Sztompka, 1999; Möllering, 2006). Such studies typically suggest that trust brings improvement in job satisfaction, job performance, and employee commitment (Robinson, 1996; Dirks & Ferrin, 2001); leads to faster decision-making (Shapiro, Sheppard, & Cheraskin, 1992; Fulmer & Gelfand (2012); and generates

improvements in organizational performance (Barney & Hansen, 1994). These benefits may be lost when trust in an organization is lost, which explains why literature on this subject contains various prescriptions on how to repair trust (Gillespie & Dietz, 2009; De Cremer & Desmet, 2012). Indeed, when researchers find examples of distrust they treat these as problems that need to be tackled.

Yet there exist organizations in which distrust is not only allowed to stay, but is produced and cultivated: secret service organizations. One of the banner notices in the International Spy Museum in Washington states: "Trust No-one," and the museum collections serve as a reminder that distrust is an important operating principle in the secret service, both inside secret service organizations and between secret service organizations and other actors. Indeed, the theme of distrust in espionage is a recurrent one in spy memoirs, biographies, novels, and films. The world of spies appears to be rife with distrust, but secret service organizations have no choice in the matter. Even trusting other agents can be risky, for agents who place too much trust in their colleagues may bring about the demise of the organization if these colleagues turn out to be double-agents. Possible betrayal therefore violates the norms of trust (Collins, 2015). This is why managers in secret service organizations must endeavor to cultivate distrust—distrust in their own agents and their agents' distrust in other actors. We chose to focus on secret service organizations because they are an extreme case, or an ideal type, of distrustful organizations, but we believe that our conclusions reveal something about other types of organizations, which organizational studies scholars tend to miss.

We ask a question: How do secret service organizations produce and maintain distrust? Inspired by Actor–Network Theory (ANT), we analyzed devices, codes, rules, and procedures used in secret service organizations, and then compared them with those used in ordinary organizations. Based on our analysis, we make two contributions.

Firstly, we draw researchers' attention to distrust that is intentionally built and maintained rather than distrust that is accidental and indicative of faulty management. Secondly, we identify and discuss the material manifestations of distrust – technologies, objects and quasi-objects used by organizations to watch, listen, record, and manipulate actors both their employees and other actors. We believe that scholars studying the production and maintenance of distrust in organizations, will need to focus on technologies, physical objects, and quasi-objects. These, together with discourses, guarantee the stability of connections among organizational actions.

We begin by explaining what we mean by secret service organizations and continue with a brief review of different ways of understanding trust and distrust. After discussing the ANT approach chosen and the methods used, we present our analysis and conclusions. Before going any further, two caveats should be made. Acknowledging that there is no such thing as an *ordinary organization*, we use this term to mean organizations other than secret service organizations. Similarly, we use the word *spy*, which is a label from popular culture used to denote a wide range of roles in secret service organizations. Whereas, in practice such organizations' employees are referred to as agents, secret agents, undercover agents, intelligence officers, intel analysts, and many other terms.

Secret service organizations

Secret service organizations, also known as espionage organizations or intelligence agencies, engage in collecting, analyzing, and exploiting information in order to protect their countries from security breaches that may cause economic or political harm. Contemporary examples include the Swedish Security Service (Säpo), the UK's Secret Security Service (MI6), the US Central Intelligence Agency (CIA), and Russia's Federal Security Service (FSB). Some famous secret service organizations from the past

are the KGB in the Soviet Union (1954–1991) and the State Security Service in East Germany (Stasi, 1950–1990). People working in operational roles in secret service organizations are usually referred to as spies, secret agents, undercover officers, or intelligence officers. People who are asked why they became spies have been quoted as providing various motives: love of their country, ideological persuasion, profit seeking, satisfaction gained from deceiving others, a sense of adventure, or the seduction of danger. Some, but not all, of these motives can be shared by people joining ordinary organizations. There are also many dramatic negative consequences of being a spy: discovery, humiliation, deportation, torture, and even death. Of these possible consequences, only humiliation is to be expected in most other organizations; indeed, it is a relatively common occurrence (Czarniawska, 2008).

There have been some notable attempts to study secret organizations (in the past, Simmel, 1906; and at present e.g., Stohl & Stohl, 2011; Grey, 2012; Parker, 2018), yet field studies of the secret service are rare because, unsurprisingly, their operations are secret. In many legal frameworks, it is against the law even to acknowledge that something is secret. If investigations of practices are allowed, they are often confined to a historical perspective, such as organizational analysis of declassified material. One such study, based on already declassified material, is Chris Grey's work on Bletchley Park (2012). This was an organization dedicated to decoding—in complete secrecy. Grey described in great detail such processes as interception of signals, transmission and decryption of intercepts, intelligence assessment, secure distribution of information, and organizational arrangements that supported these processes. He explained how staff were recruited and trained, and presented various distinctions between organizational actors in Bletchley Park, such as gender, hierarchy, or social and educational background. In his discussion of the culture of secrecy, Grey highlighted the paradox of the need to

know principle—How is it known that there is a need to know? He returned to this question in his later book with Jana Costas (2016), this time focusing on two interrelated processes—ignorance and silence. These two processes, in the authors' view, produced internal boundaries between individuals and teams. Such boundaries created a complete isolation of employees, who were not allowed to discuss any aspects of their work with anyone from outside their own "compartment." Although Grey and Costas did not explicitly discuss distrust, it is implicit in their discussions of secrecy.

Erving Goffman in the introduction to his *Strategic Interactions* (1969) claimed that at the very root of distrust in secret service organizations lie interpersonal relations between spies. In order to understand how these "strategic interactions" develop, it is necessary to consider "the individual's capacity to acquire, reveal, and conceal information," claimed Goffman (1969, p. 4). His material on intelligence and espionage listed a number of "basic moves" used in interactions concerning strategic information, in which "expression games" take place. Goffman's list is obviously speculative, as an observer can never actually determine the character of the moves or the intentions behind them, but it is interesting nevertheless. What can be observed are the tools the spies are using in their interactions, and in this article we attempt a classification of what we called *devices of distrust*. Before we move on to the discussion of these devices, we briefly review the literature on trust and distrust in an organizational context.

Trust and distrust in organizations

Trust is a well-researched concept and over the past years it has attracted a number of influential reviews (see e.g., Dirks & Ferrin, 2001; Dietz & Den Hartog, 2006; Lewicki, Tomlinson & Gillespie, 2006; Schoorman, Mayer & Davis, 2007; Dirks, Lewicki, & Zaheer, 2009; Kramer & Lewicki, 2010; and Fulmer & Gelfand, 2012). Although most of these

texts have been written from a psychological perspective, there have been some notable sociological contributions to the study of trust (Luhmann, 1979; Sztompka, 1999; Bachmann, 2001; Möllering, 2001, 2006).

The definitions of trust cited most in organization studies often come from the work of Mayer, Davis, and Schoorman (1995) and Rousseau, Sitkin, Burt, and Camerer (1998). These definitions differ, but they have in common three themes: firstly, confident, positive expectations about the intentions, motives, or behavior of others (Lewis & Weigert, 1985; Rousseau, Sitkin, Burt & Camerer, 1998); secondly, willingness to be vulnerable (Mayer, Davis & Schoorman 1995; Fryxell, Dooley & Vryza 2002); and thirdly, expectation of reciprocity (Dirks & Ferrin, 2002). One limitation of these definitions is their lack of clarity as to who is the trustee, and who is the trustor, or, in other words, who trusts whom. Commenting on this lack of clarity, Lewicki and Bunker (1995) wondered whether or not trust in individuals is the same construct as trust in organized systems. Because the word *trust* is used by researchers to discuss a variety of relationships in analyses conducted at interpersonal, organizational, and societal levels, one could come to the conclusion that the phenomenon is the same across all levels. Yet it seems obvious that differences in who trusts whom (i.e. who/what are the referents of trust) can suggest different types of trust relationships (Börjeson, 2017; Fulmer & Gelfand, 2012; Zaheer and Harris, 2005).

Distrust is defined by philosophers as "lack of confidence in the other, a concern that he or she may act so as to harm us, that he or she does not care about our welfare, intends to act harmfully, will not abide by basic moral norms, or is hostile towards us" (Govier, 1997, p. 34). There is less agreement among researchers on how distrust is related to trust. The recent literature on distrust is concerned with the question—Are

trust and distrust symmetrical concepts i.e., are they opposites of each other, or can they occur simultaneously?

Lumineau (2017) identified the two main, yet contradictory, approaches to conceptualizing distrust in organization studies' literature. The first approach assumes that trust and distrust are one-dimensional and at opposite ends of the same continuum—that they are mutually exclusive (e.g., Deutsch, 1958; Hosmer, 1995; Lewicki & Bunker, 1996; Schoorman, et.al., 2007). In this conceptualization, "low trust" is perceived as equivalent to "high distrust," and high trust equivalent to low distrust (Bigley & Pearce, 1998). Saunders et al. (2014) refer to this as an "either/or" relationship.

The second approach, the so-called bi-dimensional model, assumes that trust and distrust are conceptually distinct constructs, which exist on two separate continua, and can increase and decrease independent of each other (Luhmann, 1979; Lewicki et al., 1998). In other words, trust and distrust can co-exist in the same relationship (McKnight and Chervany, 2001; Saunders, et al. 2014). Lewicki et al. (1998) explained this relationship as follows: "just as it is possible... to like and dislike, and to love and hate, it may be possible to trust and distrust others" (1998: 449). Moreover, Lewicki et al. (1998) argued that the either/or view does not capture the complexity of the employment relationship, and that it is possible for an individual to experience one of four relationship conditions: low trust/low distrust, high trust/low distrust, low trust/low distrust, and high trust/low distrust. Saunders et al. (2014), in their mixed-methods study, found that trust and distrust judgments rarely occur simultaneously with regard to a single trustee subject, and that absence of trust is not the same as distrust. They concluded that when employees are distrustful and managers wish to reduce this distrust, they need different interventions from those used to build and maintain trust.

The complex relationship between trust and distrust was acknowledged by Niklas

Luhmann:

> ... trust depends on the inclination toward risk being kept under control and on the quota of disappointments not becoming too large. If this is correct, then one could suppose that a system of higher complexity, which needs more trust, also needs at the same time more distrust, and therefore must institutionalize distrust, for example in the form of supervision. (Luhmann, 1979: 89)

We acknowledge the complexity of the conceptualizations of trust and distrust, and in line with the bi-dimensional perspective on trust and distrust, we believe that in secret service organizations trust and distrust co-exist and are both crucial to the functioning of such organizations. If spies were not able to gain the trust of others (e.g., their informants), they would not be able to do their job. Also, to do their job, they sometimes have to trust their agents. At the same time, however, spies are taught to distrust as trusting too much places them in danger.

In our study, we specifically focused on distrust, and we chose to work with the concept of distrust that takes into account both interpersonal relations and organizational systems (Grey & Garsten, 2001). We are interested in exploring a range of distrust relationships: (1) distrust between spies, (2) distrust between spies and ordinary people, (3) spies' distrust of their bosses, and (4) bosses' distrust of their agents.

Actor–Network perspective on distrust

How do secret service organizations produce and maintain distrust? Attempting to answer this question, we took inspiration from scholars of science and technology (e.g., Latour, 1992), who reminded organization scholars of the importance of objects and quasi-objects in the production and maintenance of social connections. In order to incorporate these important insights, we applied Actor–Network Theory (ANT, which, in

spite of its name, is not a theory but an approach to studying collective action, Latour, 2012).

The ANT approach does not suggest turning away from studying discourses—after all, its main inspiration has been the work of the semiotician Algirdas Julien Greimas (see e.g., Greimas, 1990; Latour, 1992). Instead it suggests that words and things, humans and nonhumans must be studied together, and with equal attention. Thus, John Law and Annemarie Mol (1995) spoke of "semiotics of materiality," and the Montreal School of Communication showed convincingly that things speak, and texts do things (see e.g., Cooren, 2009; Robichaud, & Cooren, 2013). Utterances make a difference (see Austin, 1962/1975), but turned into texts become quasi-objects, and their impact is stronger and much longer (Ricoeur, 1981). In organizations, words are used to control people and things, but things are also used to control words and people (Czarniawska-Joerges & Joerges, 1988).

Thus inspired, we began by analyzing devices, codes, rules, and procedures employed in secret service organizations for control purposes. Having analyzed them, we asked the next question: Do these devices, rules, and procedures differ from those used in *ordinary* organizations? After all, Kramer had already noted in 1999 that distrust and suspicion are common, recurring problems in many organizations. So why is there so much attention accorded to trust and so little to distrust?

One of the reasons could be the well-entrenched tradition of conducting asymmetrical studies (more on that topic in Latour, 1987). Management and organization studies have long been either eulogical (based on the assumption that distrust is proof of broken trust that needs to be immediately repaired, see e.g., Gillespie & Dietz, 2009; Bachmann, et al., 2015) or critical (based on the assumption that distrust is inherent in contemporary employment relationships and that nothing can be done about it). One

example of the inherent distrust model was provided by Alan Fox (1974), who argued that employment is an entirely unequal relationship, characterized by domination, and that it exists solely to satisfy the interests of the dominant party: the employer.

Only recently have symmetrical studies become more common, and organization scholars have started to examine the concept of distrust in greater detail (see e.g., Tanghe et al., 2010; Lumineau, 2017; Saunders et al., 2014). Like us, some of these scholars see value in examining distrust not solely in relation to trust, but also as a concept in its own right (Hardin, 2004). Also, the possibility of a loose coupling between the two has been suggested by Lumineau (2017), who noted that the absence of trust does not imply a high level of distrust and vice versa. Yet, despite this increasing recognition of the importance of studying distrust, many issues surrounding distrust remain under-explored, such as, the possibility—shocking as it may seem—that distrust may be not only a "destructive force" (Bijlsma-Frankema et al., 2015: 1018) but also straightforwardly constructive.

Building on the earlier attempts to study secret organizations (Simmel, 1906; Stohl and Stohl, 2011; Grey, 2012; Parker, 2016) and conceptualizations of secrecy in a variety of non-secret organizations (Costas & Grey, 2013; 2016), we focused on an in-between situation: organizations that are not secret but the affiliation of certain people is enshrined in secrecy. Following the growing tradition for applying the ANT approach to organization studies (see e.g., Czarniawska & Hernes, 2005; Belliger & Krieger, 2016), we analyze devices and quasi-objects used by organizations to create and maintain distrust and secrecy.

Research design

Our focus on devices of distrust led to us adopting the unusual approach of visiting three museums of secret-service organizations: German Spy Museum in Berlin, International

Spy Museum in Washington, and National Cryptologic Museum in Annapolis. The museum collections are open to the public, and two of the museums have commercial intent and charge an entrance fee, while the one located inside the National Security Agency is free. In contrast to corporate museums, which are exhibit-based facilities owned and operated by a company (e.g. Stigliani & Ravasi, 2007), these three museums collect and display objects from the archives that illustrate the history of various security agencies and their operations. These collections are not confined to the two countries in which the museums are located as they include artifacts used in a number of secret service organizations: KGB, MI5, MI6, and Stasi. The artifacts are of historical value, and range from the 19th century US cipher machines to devices used by the Stasi in the 1980s. For obvious reasons, an analysis of devices currently used by spies would not be easy to perform. Also, as far as we know, these are the only spy museums in the world.

The two spy museums house thousands of artifacts that capture the most dramatic moments in the history of secret service organizations and the spy profession. These collections contain devices developed and used by spies, as well as descriptions of the techniques they employed and places they worked. At the National Cryptologic Museum the collections capture the legacy of the cryptologic profession. All three of these museums display artifacts that illuminate the work of famous spies and their achievements, illustrate the milestones in secret service operations, document famous espionage actions, and reveal strategies and tactics used in the most secretive missions in world history. In contrast to corporate museums, the three museums are less focused on the employees of secret service organizations, but appear to be designed for the lay visitor. The exhibits' descriptions are written in accessible language with no technical jargon, and do not assume any understanding of the historical contexts in which the objects were used.

In all three museums, visitors are told that the collections were prepared and maintained with the advice and assistance of experts in the intelligence community. All three places are advertised as educational facilities, allowing people to learn about the history of espionage and its role in influencing political decisions. The text on the International Spy Museum's website states that the museum is "committed to the apolitical presentation of the history of espionage in order to provide visitors with nonbiased, accurate information." The National Cryptologic Museum website claims to promote "the possibility of exciting jobs in an area they [the visitors] may not have thought possible."

Because all three museums are open to the public, no special permission was sought for access. All three museums either gave us permission to photograph exhibits or allowed us to use their own stock photographs in publications. Repeated visits were made to the museums to photograph most of the artifacts and study their descriptions, in order to identify their functions and the circumstances for which they were designed.

The analysis followed the usual abductive pattern, going back and forth between field material and relevant theoretical insights (see e.g., Eco, 1990). The first stage of the analysis involved identifying the function of the artifacts on display. In order to facilitate our orientation within the contents of the enormous collections, we classified the objects into categories guided by the question—What were the objects used for? Based on the emerging functions, we classified the objects into categories that we reviewed by focusing on the question—How do they relate to maintaining distrust in secret service organizations? For example, we asked the following questions: what the use of a certain object tell us about the relationship between people? Does the use of these objects and quasi-objects suggest a conscious choice to distrust? Not all artefacts in the museums related to distrust (for example modes of transport used by spies, or cards containing

stories of historical spy operations), and we excluded these from the analysis. The artefacts which related to distrust we classified the objects into types of devices, for example concealment devices, recording devices, concealed photography devices, or break-in devices. The full classification of the devices of distrust is included in Table 1. The results of our analysis i.e., the classification of the devices and their functions, were later verified in a discussion with an ex-employee of a secret service organization. The purpose of this discussion was to verify our understanding of these artifacts, and corroborate the validity of our classification.

We were also able to identify a number of quasi-objects, such as codes, rules, and procedures used in secret service organizations, presented by the museums in the form of textual descriptions accompanying the artifacts and recorded voice memos. For example, pressing a button next to an exhibit activated a pre-recorded voice explaining the object's function. Sometimes it was the voice of an unknown narrator, other times it was a famous person from the world of espionage.

One—inevitable—limitation of our approach is that the devices displayed and listed here are part of historical collections, and may be perceived as outdated. However, the technological details were not of concern for this project, and instead we focused on their rationale and the functions that they performed. Arguably, these functions have not changed over time. Contemporary spies no doubt use new devices and appropriate new technologies relevant to emerging threats. The museums were not displaying these devices, but emphasized the importance of new technologies:

> With advancement in technology, secure telephony became portable, first fitting in a briefcase, and finally in a pocket. The cryptographic methods improved as well. Today, mathematical algorithms encrypt phone calls made by the President and other government leaders. (Text accompanying a picture of G. W. Bush making a phone call, National Cryptologic Museum).

Because ordinary organizations are far more researched than secret service organizations, in the second stage of our analysis, we drew from existing academic and popular literature on contemporary organizations. With the help of this information, we attempted to pair secret organizations' devices of distrust with those in use in ordinary organizations. The match is not complete, but it is a promising start.

Devices in use in secret organizations

Among the most-used artifacts were *recording devices*, which had different forms that changed over time and with technological advances. Bugging devices and secret recording devices were typical between 1960 and 1980, and changed into various forms of electronic surveillance in the digital era. These original devices were hidden in a multitude of objects: watches, match boxes, cigarette lighters, briefcases, umbrellas, and even bras (Photos 1, 2 and 3). Although they served as an obvious device for saving information, they were also used for blackmail and in other situations in which trust is betrayed—either by the people recorded or by those who recorded them without their knowledge.

Place photos 1, 2 and 3 about here

The museum collections house a range of objects used to *break into* and *break out* of places—pins for unlocking doors, wrenches, devices to disable alarm systems, and instruments that detect the vibrations of an intruder's footsteps and send signals to an earpiece. Spies were also known to use various ways *of hiding* themselves—in concealed compartments in cars and rooms, and using thermal blankets to mask their body heat

and avoid detection.

The extreme end of the tools of the trade is reserved for a variety of *weapons* imaginatively hidden in everyday objects—pistols designed to fire at close range and concealed in lipsticks, cigarette lighters, or pipes; small blades hidden behind lapels, to allow hand-to-hand defense in emergencies; and a range of booby-trap explosive devices. Pride of place in both the Washington and Berlin museums is reserved for umbrellas containing poison gas pellets that leave no trace of their deadly presence on the human body (Photo 4).

Place photo 4 about here

Lie detectors were designed and are used with the principle of distrust in mind. They are supposed to determine if a person is telling the truth, by testing for physiological changes normally associated with lying. More extreme methods than a lie detector for extracting secrets from agents exist of course, in the form of torture. To counteract the threat of torture, and thus escape the risk of revealing valuable information to the enemy, *suicide pills* were invented. They came in two forms: real suicide pills that an agent can take if captured by the enemy, and placebo suicide pills used to test the loyalty of an agent in situations fabricated by the agencies. The loyal agent is expected to commit suicide rather than disclose information or undergo torture. The necessity of both types of pills was based on distrust—the agency's distrust of the agent's ability to withstand torture and to choose an easy death over the risk of torture.

The list of objects used *to disguise* a spy is a long one: clothes that create fake identities, false beards, and wigs being the most obvious. A 1944 US spy government manual advised "Never use a disguise except as a last resort – but when you do, play it for

what it's worth." Disguises, however, are not expressions of distrust of the secret service towards their employees; they are expressions of distrust towards other people and other organizations.

Perhaps the most prominent quasi-objects are codes and their necessary counterpart: *code-breaking software* (Photo 5).

Place photo 5 about here

Special transmission equipment is used to encrypt messages and decipher them at the receiving end. One half of cryptology is about studying secret messages and breaking the system; the other half is about using methods or systems to change the text to hide its real meaning. The Cryptologic Museum contains an impressive collection of cypher discs (first invented in Italy in the 15th century), cypher machines, alphabet strips, and encryptors.

Quasi-objects: Codes, rules, and procedures in secret organizations

As for *quasi-objects* (Latour [2005, p. 238] also spoke of "quasi-subjects," which could be a good term for fake identities), it needs to be remembered that the work of spies is made possible because they have fake identities. A *cover* is the creation of a new persona that guards and conceals the real identity of the spy. It is a quick disguise that sometimes consists merely of a false name. A *legend* is a carefully developed artificial life history and background description, both requiring painstaking attention to detail. A spy may live a false identity for years, actually establishing the legend in preparation for an operation.

Coding is a way of securing military, diplomatic, business-related, and other sensitive types of communication from interception by competitors, the enemy, or even

innocent bystanders (Czarniawska, 2014). In his analysis of Bletchley Park's operations from the point of view of organization theory, Chris Grey (2012, 269) suggested that even organization studies "encode" organizations "by the deployment of arcane vocabulary and also through the straitjacket of typologies, ideal types, concepts and constructs which do not necessarily assist the understanding of 'how things work in organizations'." Codebreaking did not end with World War II, but it is currently perceived quite differently. Codebreakers were "good guys"; hackers—the present-day codebreakers—are now increasingly seen as "bad guys" (Halpern, 2012).

But there are also codes of conduct that describe—and regulate—the way people are to be treated and products are to be used. The rules and procedures used by spies are part of their tradecraft —"the tools and techniques that influence battles and sway governments" (International Spy Museum).

From a whole array of rules and procedures, we have chosen to present the best known and most central to the functioning of secret organizations, the most famous of which is the *need-to-know* rule. As Goffman (1969, p. 78–79) noted, "[i]nformation is the hardest to guard, since it can be stolen without removing it." This is why secret service organizations operate on the basis of reducing channels of communication. Goffman referred to this process as "compartmental insulation" (ibid).

Secret service organizations often operate on the basis of a network in which the agents are *nodes*, and they connect with a limited number of other nodes without knowing the whole network. Agent runners play a crucial role in this organization, as they are often the only contact with the secret organization; all orders and instructions come from them. In contrast to ordinary organizations and other actor–networks, in which a spokesperson plays the central role (Latour, 1988), those who speak publicly in secret organizations are detractors; the others whisper. Distrust underpinned by the

requirement of absolute secrecy is evident in the notices in some of the 1940s posters and manuals: “Rumors cost lives”; “A careless word… needless sinking”; “Loose lips might sink ships”; “Someone talked!” These were often accompanied by an image of the disastrous consequences of indiscretion—a sailor drowning in the ocean, with a sinking ship in the background.

Goffman (1969) also noted that ignorance makes people incapable of betraying their own interests. This principle underpins one of the main rules of secret service operations. The consequences of revealing information are disastrous, so the need-to-know principle was necessary; some of the human sources whose identity the principle is meant to protect could be at risk of imprisonment or death should their activities be revealed. Even when spies obtain secret information from the enemy, they are often not allowed to reveal this fact to the enemy—what Goffman called a “counter-uncovering” move. When the Bletchley Park scientists broke the Enigma code, they still could not avert all Nazi attacks, as this would alert the enemy that the code had been broken. Instead they selectively averted attacks, allowing the Nazis to carry out some of their attacks in order to maintain the Allies’ cover (Grey, 2012). Lives were sacrificed in order to prevent the enemy from discovering that the codes had been broken.

Recruitment procedures are another illustration of the principle of distrust. Recruitment of trustworthy spies is based on the candidates' capacity for ultimate distrust; it requires a thorough verification of the suitability of candidates and their ability to distrust others. Candidates are treated with suspicion and are expected to be suspicious of everything. Verifying the suitability of spies happens through the process of vetting. The secret service organization needs to have information about all aspects of a potential recruit’s life, in order to avoid the risk of blackmail and bribing. Goffman noted that intelligence agents are often chosen from among people whose past and present

offer the fewest bases for mobilizing divergent interests (1969, p. 42). Vetting is crucial in espionage, and would-be agents (and their family and close friends) who have not been properly assessed for their ability to keep secrets cannot be recruited.

Along with coding and decoding devices, spies are said to use certain *procedures to exchange information*. Visitors to the spy museums are reminded that espionage is primarily about stealing information without being noticed and passing it on without interception. Miniature texts can be placed on such unobtrusive objects as the underside of a postage stamp and deposited in *dead drops* (sometimes by means of dead-drop spikes— best described as hollows nail that can hold pieces of paper and be inserted into the ground) in prearranged locations in isolated places. The receiver reads these messages by means of a microdot viewer. The spies then use predetermined signs to let others know about a new or completed operation; these signs are called signals and can be items or marks placed somewhere—a chalk mark on a postbox, for instance.

Thus, the underpinning principle of spy operations is distrust. How about organizations that claim that the underpinning principle of their operation is trust? We now attempt to show a contrast to the usual assumption that distrust, if discovered, must be reduced or removed (see e.g., Saunders et al., 2014; Gago-Rodrigues & Naranjo-Gil 2016), whereby trust can be intentionally produced and maintained.

Distrust in ordinary organizations

Our investigation of the devices of distrust in secret service organizations inspired us to consider whether such devices exist in ordinary organizations. It can be claimed that the very beginning of scientific management was also the beginning of the introduction and gradual improvement of distrust devices in ordinary organizations. After all, time clocks forcing employees to clock in and out for their shifts could hardly be seen as an expression

of trusting the workers (see e.g., Luhmann, 1979). Historically, Fox (1966) argued, distrust or "low trust" initiatives were related to "low-discretion" jobs, characterized by greater direct and indirect control of the individual worker. A closer look at the contemporary organization, however, suggests that "high discretion" jobs—those of professionals, such as lawyers or doctors (Siebert et al., 2015), or employees in knowledge-intensive industries—are characterized by equally high levels of control of employees. Even working from home, often presented as an example of empowerment providing employees with the discretion to decide their mode and time of working, can be closely monitored by electronic communication (Fairweather, 1999; Taskin & Edwards, 2007). Another good example is the GPS with a recorder, often installed in company cars to allow employers to know the whereabouts of an employee.

More and more sophisticated technologies (i.e., so-called *spyware*) are being employed at the service of surveillance (Taylor & Bain, 1999; Bain & Taylor, 2000; Kinnie, et al. 2000; Lankshear, et al. 2001; Mulholland, 2004; Ball, 2010). There are recording and surveillance devices everywhere, and they serve as an expression of distrust of both outside agents (robbers, hackers) and disloyal employees. Indeed, surveillance is currently one of the hottest topics for debate both in the popular press and in management literature (see e.g., Lyon, 2007; Ball & Margulis, 2011; Allmer, 2012; Haque, 2015). Manifestations of distrust through surveillance involve monitoring employees' telephone and e-mail communications or protecting access-to-information systems through passwords. Another example is restricting physical access to certain parts of a building to those with magnetic card passes or master keys (Lashinsky, 2012). This phenomenon could be (and is) interpreted as a breakdown of trust in society or, alternatively, as an institutionalization of organizational distrust.

As with lie detectors, there are some non-secret organizations that may use

surveillance devices and resort to certain rules and procedures of distrust—undercover police, crime detectives, or special forces. Even without a specific device, it is still possible to detect lies by using verbal tricks e.g., setting a trap for interviewees in selection interviews. In fact, some management websites offer practical advice on how to detect lies in the responses of interviewees.[1] Moreover, the principle of distrust is often built into recruitment, selection, and induction procedures. Silverman and Jones (1976) showed convincingly how recruiters—intentionally or unconsciously—exclude candidates from specific social backgrounds. As they put it,

> ... "acceptable" people are people who play the game recognizably well and are rewarded for it. Yet this presumes a game-known-in-common, with moves available to be performed and observed by players. So, as well as playing the game at a high standard, there is also the issue of playing the game at all. (1976, p. 117)

Clearly, "playing the game well" and using Goffman's counter-uncovering moves is not limited to secret organizations. Many recruitment interviews, and even performance-appraisal meetings, can often take a form that closely resembles interrogation.

Fabricated identities are the normal content of websites, including legends concerning founders or leaders of organizations. Like spy legends, they can be undermined. Also, selection and recruitment panels are on the lookout for fabricated identities and legends of applicants for jobs. Just like spy legends, these can be undermined by checking letters of reference against several sources—yet another procedure of distrust evident in contemporary organizations.

---

[1] https://www.linkedin.com/pulse/how-tell-candidate-lying-interview-ji-a-min-masc, accessed 2016-10-26.

Secrecy, distrust, and the use of various devices to protect information are clearly visible in the launching of new products and the adoption of new strategies. These are also inherent in contract negotiations in commercially sensitive inter-organizational deals. The need-to-know rule is familiar to all organizations. Economic espionage and the protection of trade secrets are well-known activities, supported by a solid legal base (Snider & Ellins, 2006). Pendergrast's (2000) famous book explaining how Coca-Cola preserved its secrets can compete with many secret service stories. In *Inside Apple*, Lashinsky (2012) revealed that employees were kept in the dark about new Apple products, just as the public was. Apparently, they were allowed to enter only certain parts of Apple's campus that directly related to their work. What is more, according to Lashinsky, it was not uncommon for employees to have access to a room that their boss could not enter, and it was not common to question this procedure. "What you're not told, you don't ask about," seemed to be the leading maxim in Steve Job's "embrace secrecy" formulation. Apple was, in the words of one employee, "the ultimate need-to-know culture" (Lashinsky, 2012, p. 41).

Ordinary organizations do not use suicide pills (as far as we know!), yet an involuntary resignation from a senior post could be seen as a metaphorical suicide pill. And so are symbolic executions which resonate with spy executions:

> … the security briefing, the one element that no Apple employee forgets. Call it Scared Silent. Borchers, the iPhone marketing executive who had worked at Nike and Nokia before joining Apple, recalled the scene. "Whoever headed up security came in and said, 'Okay, everybody understands secrecy and security are incredibly important here. Let me just explain why.' And the rationale is that when Apple launches a product, if it's been a secret up until the launch, the amount of press and coverage and buzz that you get is hugely valuable to the company. 'It's worth millions of dollars', I remember her saying." So there's no confusion, the

> penalty for revealing Apple secrets, intentionally or unintentionally, is clear: swift termination. (Lashinsky, 2012, 36)

Apple is not unique: as Anteby (2014) reported, the metaphor of "Russian roulette" has been used often when speaking of non-tenure decisions. But we do not wish to extend the analogy too far. Table 1 contains some comparisons, although a match-for-match comparison of devices of distrust in secret services and ordinary organizations is not always possible. Secret service organizations are, of course, a special case, an extreme case of the production and maintenance of distrust. Yet our analysis of devices, rules, and procedures of distrust in secret service organizations allowed us to draw some conclusions about trust and distrust in ordinary organizations. Some of these devices have been discussed in literature on control and surveillance in organizations, but they are conspicuously absent from the literature on trust and distrust.

Table 1 here

Distrust in secret and ordinary organizations

Through our analysis of the devices of distrust in secret service organizations, we have made two contributions to organizational theory: first is about the extent to which distrust is integral to many intra- and inter-organizational relationships, and second in relation to the use of Actor-Network Theory in analyzing distrust. We discuss these two contributions in turn now.

The literature on secret service organizations, both academic and popular, suggests that spies at the same time appear to trust and distrust each other, their organizations, and others, and both trust and distrust are integral to the functioning of

the secret service organizations. But, as secret service organizations are an extreme case of distrustful organizations, in this paper we have specifically focused on distrust. Inspired by ANT, we analyzed the devices, codes, rules, and procedures used in secret service organizations, and we asked another question: Do these objects and quasi-objects differ from those used in ordinary organizations?

It seems that the functioning of secret service organizations may prove more relevant to an understanding of ordinary organizations than is usually assumed (see Costas & Grey, 2016, and Parker, 2016, on analysis of secret organizations). One obvious explanation for the connection between the two types of organizations is the technology transfer. Most organizational technologies came to civil organizations from the military, and the secret service organizations searched for and applied the most advanced (or better said, extreme) examples of these military technologies. For the latter, those that worked were then transferred to ordinary organizations in a milder form.

This relevance becomes obvious in the light of the fact that the literature on organizational trust suggests that trust is necessary for the functioning of most, if not all, organizations. Creating, maintaining and repairing trust seems to be only option to pursue by contemporary organizations (Börjeson, 2017; Fulmer & Gelfand, 2012; Reich-Graefe, 2014). This approach to trust-as-choice was critiqued by Zygmunt Bauman (2010, 30) who wrote: "That it is by trust that the economic, political and social orders stand, and that it is by its absence that they fail has now become the doxa of political science." Organizational trust has evolved into an industry; armies of academics and consultants advise organizations on the building and maintaining of trust, and how to repair it when it is broken. *Trust* is a word that looms large in management and organization studies, and has, over the years, overshadowed such terms as loyalty, engagement, and commitment.

Yet, the quote from Niklas Luhmann which we included in our introduction, points out the complex connection between trust and distrust in complex systems. This point made by Luhmann seems to have been ignored by contemporary trust researchers. Yet, as we have demonstrated, organizations built primarily on distrust do exist, and quite a few elements of distrust are built into ordinary organizations as well. A lack of confidence in the other or a concern that he or she may want to harm us, referred to by Govier in his definition of distrust, can be found in most organizations—secret or not.

Many researchers have studied trust (e.g., Sitkin & Stickel, 1996; Grey & Garsten, 2001; Appelbaum, et al., 2004; Godard, 2004; and Elsbach et al., 2012); but distrust is often be described as accidental, in many cases as unintended and, in the worst case, proof of faulty management. In contrast, our study redirects attention to distrust that is intentionally built and maintained, as seen in the Apple example. It is the cornerstone of some organizations, and the basis for their success: as Luhmann rightly pointed out, it is institutionalized. Secret service organizations would endanger the lives of many people if they ceased to distrust potential recruits, their employees, and strangers from outside their own circles. But in the same way, the operations of some knowledge-intensive and patent-based organizations would risk their competitive advantage if they were more trusting and open about their commercial secrets. It could be said that this mixture of trust and distrust has become much more visible at present in “the new technological age” of information (Merges et al., 2012), but historical material could also be helpful in understanding contemporary phenomena.

Actor-Network Theory has never been used in the study of distrust, where the role of artifacts did not seem obvious, but it is an excellent frame for analyzing distrust, in whose construction artifacts pay a crucial role. Previous studies treated distrust as "a state with cognitive and affective dimensions" (Saunders, et al, 2014, Bijlsma-Frankema,

et al. 2015), but entirely ignored the material manifestations of distrust. Our study demonstrates the power of these material manifestations. The presence of objects and quasi-objects reminds organizational actors that they are being watched, listened to, recorded, and manipulated; in other words, that they are distrusted. The presence of these objects and quasi-objects also allows organizational actors to watch, listen, record, and manipulate others. In future studies of production and maintenance of distrust in organizations, it is necessary to focus on technologies, physical objects, and quasi-objects, as these reflect individuals' conscious choices to distrust, and to organize action around distrust. These objects and quasi-objects, together with discourses, guarantee stability of the connections among organizational actions.

References

Allmer, Thomas (2012). *Towards a critical theory of surveillance in informational Capitalism*. Frankfurt am Main: Peter Lang.

Anteby, Michel (2013) Manufacturing Morals: The Value of Silence in Business School Education, Chicago: University of Chicago Press.

Appelbaum, Eileen; Batt, Rosemary, & Clark, Ian (2013). Implications of financial capitalism for employment relations research: Evidence from breach of trust and implicit contracts in private equity Buyouts. *British Journal of Industrial Relations,* 51(3): 498–518.

Austin, John (1962/1975). *How to do things with words*. Cambridge, MA. Harvard University Press.

Bachmann, Reinhard (2001). Trust, power and control in trans-organizational relations. *Organization Studies*, *22*(2), 337–65.

Bachmann, Reinhard; Gillespie, Nicole, & Priem, Richard (2015). Repairing trust in organizations and institutions: Towards a conceptual framework. *Organization Studies,* 36(9): 1123–1142.

Bain, Phil & Taylor, Peter (2000). Entrapped by the "electronic panopticon"? Worker resistance in the call centre. *New Technology, Work and Employment*, 15(1): 2-18.
Ball, Kirstie S. (2010) Workplace surveillance: An overview. *Labor History*, 51(1): 87–106.

Ball, Kirstie S. & Margulis, Stephen T. (2011) Monitoring and surveillance in call centers: A review and synthesis. *New Technology, Work and Employment*, 26(2): 113–126.

Barney, Jay B., & Hansen, Mark H. (1994). Trustworthiness as a source of competitive advantage. *Strategic Management Journal, 15*(S1), 175-190.

Bauman, Zygmunt (2010). *This is not a diary*. Cambridge, UK: Polity Press.

Belliger, Andréa & Krieger, David J. 2016. *Organizing networks. An actor-network theory of organizations.* Bielefeld: transcript Verlag.

Bigley, Gregory A. & Pearce, Jone L. (1998). Straining for shared meaning in organisational science: Problems of trust and distrust. *Academy of Management Review* 23(3), 405-21

Bijlsma-Frankema, Katinka; Sitkin, Sim B. & Weibel, Antoinette (2015). Distrust in the balance: The emergence and development of intergroup distrust in a court of law. *Organization Science*, 26(4): 1018–1039.

Börjeson, Love (2017) Trust and betrayal in interorganizational relationships: A systemic functional grammar Analysis. Human Relations, 71(3): 399-426

Boyd, William (2006). *Restless*. London: Bloomsbury.

Child, John & Rodrigues, Susanna B. (2004). Repairing the breach of trust in corporate governance. *Corporate Governance: An International Review,* 12(2): 143–152.

Collins, Alan (ed.) (2015) *Contemporary Security Studies*, Fourth Edition, Oxford: Oxford University Press.

Cooren, François (2009) Textual agency: How texts do things in organizational settings. *Organization*, 11(3): 373–393.

Costas, Jana & Grey, Chris (2014). Bringing secrecy into the open: Towards a theorization of the social processes of organizational secrecy. *Organization Studies*, 35(10): 1423–1447.

Costas, Jana & Grey, Chris (2016). *Secrecy at work. The hidden architecture of organizational life*. Stanford, CA: Stanford University Press.

Czarniawska, Barbara (2008). Humiliation: A standard organizational product. *Critical Perspectives on Accounting*, 19: 1034–1053.

Czarniawska, Barbara (2014). Codification of everything? In: Pallas, Josef; Jonsson, Stefan and Strannegård, Lars (eds.) *Organizations and media – organizing in mediatized world,* pp. 132–144*.* London: Routledge.

Czarniawska, Barbara & Hernes, Tor (eds.) (2005). *ANT and organizing*. Malmö/Copenhagen: Liber/CBS Press.

Czarniawska-Joerges, Barbara & Joerges, Bernward (1988) How to control things with words: Organizational talk and control. *Management Communication Quarterly*, 2(2), 170–193.

De Cremer, David, & Desmet, Pieter (2012). Restoring trust depends on the victim's motives: A motivated trust repair model. In: Roderick M. Kramer and Todd. L. Pittinsky (eds.) *Restoring Trust in Organizations and Leaders: Enduring Challenges and Emerging Answers* (pp. 241-256). New York, NY: Oxford University Press, Inc.

Deutsch, Morton (1958). Trust and suspicion. *Journal of Conflict Resolution*, 2:265–279.

Dietz, Graham, & Den Hartog, Deanne N. (2006). Measuring trust inside organisations. *Personnel Review, 35*(5), 557–588

Dirks, Kurt T., & Ferrin, Donald L. (2001). The role of trust in organizational settings. *Organization Science,* 12: 450–467.

Dirks, Kurt T.; Lewicki, Roy I.; & Zaheer, Akbar (2009). Repairing relationships within and between organizations: Building a conceptual foundation. *Academy of Management Review,* 34: 68–84.

Elsbach, Kimberly D.; Stigliani, Ileana & Stroud, Amy (2012). The building of employee distrust: A case study of Hewlett-Packard from 1995 to 2010. *Organizational Dynamics*, 41(3): 254–263.

Fairweather, N. Ben (1999). Surveillance in employment: The case of teleworking, *Journal of Business Ethics*, 22(1): 39–49.

Fox, Alan (1966). *Research papers 3: Industrial sociology and industrial relations*. London, UK: Her Majesty's Stationery Office.

Fox, Alan (1974). *Beyond contract: Work, power and trust relations.* London: faber & faber.

Fryxell, Gerald E.; Dooley, Robert S., & Vryza, Maria (2002). After the ink dries: The interaction of trust and control in US–based international joint ventures. *Journal of Management Studies*, *39*(6), 865–886.

Fulmer, C. Ashley, & Gelfand, Michele J. (2012). At what level (and in whom) we trust across multiple organizational levels. *Journal of Management, 38*(4), 1167-1230

Gago-Rodriguez, Susana & Naranjo-Gil, David (2016). Effects of trust and distrust on effort and budgetary slack: and experiment. *Management Decision*, 54(8): 1908–1928.

Gillespie, Nicole & Dietz, Graham (2009). Trust repair after an organization-level failure. *The Academy of Management Review*, 34(1): 127–145.

Goffman, Erving (1969). *Strategic interaction*. Philadelphia, PA: University of Pennsylvania Press.

Greimas, Algirdas Julien (1990) *The social sciences: A semiotic view*. Minneapolis, MN: The University of Minnesota Press.

Grey, Chris (2012). *Decoding organization: Bletchley park, codebreaking and organization studies*. Cambridge: Cambridge University Press.

Grey, Chris & Garsten, Christina (2001). Trust, control and post-bureaucracy. *Organization Studies,* 22(2): 229–250.

Govier, Trudy (1997). *Social trust and human communities.* Montreal, QC: McGill-Queen's Press.

Halpern, Sue (2012). Are hackers heroes? *New York Review of Books*, LIX (14): 42–45.

Haque, Akhlaque (2015). *Surveillance, transparency and democracy: Public administration in the information age*. Tuscaloosa, AL: University of Alabama Press.

Hardin, Russell (2004). *Distrust: Manifestations and management* (Third edition). New York: Russell Sage Foundation.

http://www.bbc.com/news/world-europe-28001780, accessed 2016-10-18.

https://www.linkedin.com/pulse/how-tell-candidate-lying-interview-ji-a-min-masc, accessed 2016-10-26.

Hosmer, LaRue Ton (1995). Trust: The connecting link between organizational theory and philosophical ethics. *Academy of Management Review,* 20(2): 379–403.

Kinnie, Nick; Hutchinson, Sue & Purcell, John (2000). "Fun and surveillance": the paradox of high commitment management in call centres. *International Journal of Human Resource Management*, 11(5): 967-985.

Kramer, Roderick M. (1999). Trust and distrust in organizations: emerging perspectives, enduring questions. *Annual Review of Psychology*, 50(1): 569–598.

Kramer, Roderick M., & Lewicki, Roy J. (2010). Repairing and enhancing trust: Approaches to reducing organizational trust deficits. *The Academy of Management Annals*, 41: 245–277.

Lashinsky, Adam (2012). *Inside Apple. How America's most admired – and secretive – company really works.* London: John Murray.

Latour, Bruno (1987). *Science in action: how to follow scientists and engineers through society.* Cambridge, MA: Harvard University Press.

Latour, Bruno (1988). *The Pasteurization of France*. Cambridge, Mass., Harvard University Press.

Lankshear, Gloria; Cook, Peter; Mason, David; Coates, Sally, & Button, Graham (2001). Call centre employees' responses to electronic monitoring: Some research findings. *Work, Employment and Society*, 15(3): 595-605.

Latour, Bruno (1992). Technology is society made durable. In: Law, John (ed.) *A sociology of monsters: Essays on power, technology and domination* (pp. 103–131. London: Routledge.

Latour, Bruno (2005). *Reassembling the social*. Oxford: Oxford University Press.

Latour, Bruno (2012) "What's the story? Organizing as a mode of existence. In: Passoth, Jan-Hendrik; Peuker, Birgit; and Schillmeier, Michael (eds) *Agency without actors? New approaches to collective action.* New York: Routledge, 163–177.

Law, John & Mol, Annemarie (1995) Notes on materiality and sociality. *The Sociological Review*, 43: 274–294.

Lewicki, Roy J. & Bunker, Barbara Benedict (1996). Trust in relationships: A model of trust development and decline. In Kramer, M. Rodrick and Tyler, Tom R. (eds.) *Trust in organizations*: *Frontiers of theory and* research (pp.114–139). Newbury Park, CA: Sage.

Lewicki, Roy J.; McAllister, Daniel J.; & Bies, Robert J. (1998). Trust and distrust: New relationships and realities, *Academy of Management Review*, 23(3): 438–458.

Lewicki, Roy, J.; Tomlinson, Edward C.; & Gillespie, Nicole (2006). Models of interpersonal trust development: theoretical approaches, empirical evidence and future directions. *Journal of Management*, 32: 991-1022.

Lewis, J. David; & Weigert, Andrew (1985). Trust as a social reality. *Social Forces*, 63: 967–985.
Luhmann, Niklas (1979). *Trust and power*. Chichester: Wiley.

Lumineau, Fabrice (2017). How contracts influence trust and distrust. *Journal of Management*, 43(5): 1553–1577.

Lyon, David (2007). *Surveillance studies: An overview*. Cambridge: Polity Press.
Mayer, Roger; Davis, James H.; & Schoorman, F. David (1995). An integrative model of organizational trust. *Academy of Management Review,* 20: 709–734

McKnight David H. & Chervany, Norman L. (2001) Trust and distrust definitions: One bite at a time. In Falcone, Rino; Singh, Munindar; and Tan, Yao-Hua (eds.) *Trust in cyber-societies*. Berlin: Springer-Verlag, 27-54.

Merges, Robert P.; Menell, Peter S.; & Lemley, Mark A. (2012). *Intellectual property in the new technological age*. Alphen aan den Rijn: Wolters Kluwer.

Möllering, Guido (2001). The nature of trust: From Georg Simmel to a theory of expectation, interpretation and suspension. *Sociology,* 35, 403–420

Möllering, Guido (2006). *Trust, reason, routine, reflexivity*. Oxford: Elsevier.
Parker, Martin (2016). Secret societies: Intimations of organization. *Organization Studies*, 37(1): 99–113.

Mulholland, Kate (2004). Workplace resistance in an Irish call centre: slammin', scammin'smokin'an'leavin'. *Work, Employment and Society*, 18(4): .709-724.

Parker, Martin (2018) Employing James Bond, *Journal of Management Inquiry*, Vol. 27(2) 178 –189
Pendergrast, Mark (2000). *For God, Country and Coca-Cola. The definite history of the great American soft drink and the company which makes it.* New York: Basic Books.

Ravasi, Davide; van Rekom, Johan and Soenen, Guillaume (eds) *Organizational identity in practice*, (pp. 197–214). London: Routledge.

Reich-Graefe Rene (2014) Calculative trust: Oxymoron or tautology? Journal of Trust Research 4(1): 66–82.

Ricoeur, Paul (1981) The model of the text: meaningful action considered as text. In: Thompson, John B. (ed. and trans.) *Hermeneutics and the human sciences*. Cambride, UK: Cambridge University Press,

Robinson, Sandra L. (1996). Trust and breach of the psychological contract. *Administrative Science Quarterly,* 41: 574–599.

Robichaud, Daniel & Cooren, François (eds) (2013) *Organization and organizing: Materiality, agency, and discourse.* New York: Routledge.

Rousseau, Dennise; Sitkin, Sim; Burt, Ronald; & Camerer, Collin Farrell (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review,* 23, 393–404

Saunders, Mark NK; Dietz, Graham, & Thornhill, Adrian (2014). Trust and distrust: Polar opposites, or independent and co-existing? *Human Relations*, 67(6): 639–665.

Schoorman, F.David; Mayer, Roger; & Davis, James (2007) An integrative model of organizational trust: Past, present and future, *Academy of Management Review*, 32(2): 344-354.

Siebert, Sabina; Martin, Graeme; Bozic, Branko; & Docherty, Iain (2015). Looking beyond the factory gate: Towards more pluralist and radical approaches to inter-organizational trust research. *Organization Studies*, 36(8): 1033–1062.

Silverman, David & Jones, Jill (1976). *Organizational work*. London: Collier Macmillan.

Simmel, Georg (1906). The sociology of secrecy and of the secret societies. *American Journal of Sociology,* 11: 441–498.

Sitkin, Sim B. & Stickel, Darryl (1996). The road to hell: The dynamics of distrust in an era of quality. In: Kramer, M. Rodrick and Tyler, Tom R. (eds) *Trust in organizations: Frontiers of theory and* research (pp. 196–215). London: Sage.

Snider, Jerome G. & Ellins, Howard A. (2006). *Corporate privileges and confidential information.* New York: Law Journal Press.

Stigliani, Ileana & Ravasi, Davide (2007). Organizational artefacts and the expression of identity in contemporary museums at Alfa-Romeo, Kartell and Piaggio. In: Lerpold, Lin;

Stohl, Cynthia & Stohl, Michael (2011). Secret agencies: The communicative constitution of a clandestine organization. *Organization Studies*, 32(9): 1197–1215.

Sztompka, Piotr (1999). *Trust: A sociological theory*. Cambridge, UK: Cambridge University Press.

Taskin, Laurent & Edwards, Paul (2007). The possibilities and limits of telework in a bureaucratic environment: Lessons from the public sector. *New Technology, Work and Employment*, 22(3): 195–207.

Taylor, Phil & Bain, Peter (1999). "An assembly line in the head": work and employee relations in the call centre. *Industrial Relations Journal*, 30(2),101-117.

Zaheer, Akbar and Harris, Jared (2005) Interorganizational trust. In: Shenkar O and Reuer J (eds) Handbook of Strategic Alliances. Thousand Oaks, CA: SAGE

Table 1: Devices of distrust in secret service and in ordinary organizations

Function of distrust devices	**Examples from secret organizations**	**Examples from ordinary organizations**
Concealment	Fountain pen with a concealed microdot viewer Concealment cufflinks for storing microdots Drop-dead spikes, which could be put in the ground in prearranged places to insert hidden messages Hollow bolt used for hiding information Clams with magnets could be filled with money or cameras and attached under metal girders of bridges, etc. Microdot viewers Miniature tape recorders	Safes Password protected systems Locked rooms
Recording	Moskova recorder – could be hidden on the body and activated by the pocket controller Minifon attaché kit – a recording device concealed in a watch Wire recorders	Recorders of telephone calls (e.g. in call centres) Time clocks Smart phones used as recorders
Surveillance	Cameras hidden in spectacles, watches, briefcases, bras, and umbrellas	Security cameras GPS-systems "Spyware"
Escape	Escape map that doesn't rustle when opened Cufflink compass Pencil-clip compass Gas-tank pill which expands and blocks the fuel pipe	Escape doors (e.g. in doctors' surgeries)

	Ninisid – an instrument that can detect vibration from a vehicle or an intruder's footsteps and send an alarm in the earpiece	
Break-in	Lock picks Wrenches Burglar-alarm evasion kit	Master keys allowing entry into all offices Password bypass allowing managers access to employees' emails
Disguise	A heel-insert to change a person's walk A travel disguise kit containing comb, scissors, cold cream, tweezers, etc. False moustaches, wigs, headscarves	Dress codes in business organizations Uniforms
Hiding	Thermal blanket to mask body heat Concealed compartments in cars and rooms Shredders	Shredders
Encoding/ decoding	Cipher wheels Cipher discs Mixed alphabet strips Voice encryptors Enigma ciphers	Encrypted emails
Transport	Homing pigeons used to transport documents through the enemy lines	Special transport companies
Manipulation	Poisons and drugs used to manipulate and control the minds of people	Interview "traps"
Suicide	Cyanide tablet hidden in a molar	---
Killing	Pistol designed to fire at close range and to be concealed in a lipstick case, cigarette lighter, tobacco pipe Umbrella with poisonous gas hidden in it Booby-trap explosive devices Fire starters	---