Lund University
Department of Political Science

UNDK02
Tutor: Johan Matz

Intrapreneurs as insider threats

A Rogerian literature review

Gustav Gatu

Of course it hurts when buds burst.
Otherwise why would spring hesitate?
Karin Boye, translation Jenny Nunn

Abstract

This thesis explores how intrapreneurs can be recognized as insider threats. Nine different perspectives are presented, including deviant intrapreneurs, threatened and threatening resources, and subcultures on the tactical/operative level.

Intrapreneurs are employees who use their entrepreneurial spirit for the benefit of their organizations. Insider threats are people who, through authorized access to an organization's resources, have the potential to negatively affect the organization, its purpose and/or its stakeholders, and risk doing so. Perspectives on how intrapreneurs can be recognized as insider threats have previously been underexplored as such.

This thesis applies a Rogerian approach to find and articulate relevant perspectives in literature through thematic text analysis, as in-depth interviews and/or participatory observation of people recognizing intrapreneurs as insider threats within an intelligence community context was deemed out of scope for this thesis. Results are presented in a narrative literature review, where different perspectives are explored and cursively applied to a typical case of intrapreneurship in an intelligence community: Intellipedia.

Intellipedia is a digital information sharing platform serving the US intelligence community (USIC). It consists of three wikis that can be accessed and edited by any registered user with access. Although Intellipedia has been heralded as a success story of intra-organizational innovation, the intrapreneurs behind it have also, by their own account, been recognized as insider threats for working with the project.

Key words: Intrapreneurship, insider threats, employee deviance, intelligence services, innovation

Words: 10007

Table of contents

Definition of terms

Ambidextrous organisation: An organisation managing both exploration and exploitation (March 1991).

Efficiency-creep and **Shadow innovation**: Two separate but interrelated mechanisms that are beyond the direct control of upper managements of organizations and that constitutes enacted, rather than designed or managed, ambidexterity (Magnusson, Koutsikouria & Päivärinta 2020)

Innovation: The conception, invention *and* exploitation of new solutions (Trott 2017)

Insider Threat: Someone who, through authorized access to an organization's resources, has the potential to negatively affect the organization, its purpose and/or its stakeholders, and risk doing so.

Intrapreneurs: People who use their entrepreneurial spirit for the benefit of their employers, and whilst supported by sponsors higher up in their organization (Pinchot & Soltanifar 2021) also tend to evade their organizations' control systems and/or resource management to achieve their missions (Pinchot 1985, p. xi).

Perspective: The interrelation in which a phenomena, process or its parts are mentally viewed (Merriam-Webster, 2021)

Resources of an organization: All assets, capabilities, processes, attributes, information, knowledge, etc. controlled by the organization that enables it to conceive of and implement strategies that improve its efficiency and effectiveness (Barney 1991, p. 101, referencing Daft 1983)

Abbreviations

CIA	Central Intelligence Agency (USA)
CRGT	Critical Realist Grounded Theory
DIA	Defense Intelligence Agency (USA)
ISE	Information sharing environment
NGA	National Geospatial-Intelligence Agency (USA)
NR	Narrative literature review
NVU	New Venture Unit
STAR	U.S. House Subcommittee on Strategic Technologies and Advanced Research
TWB	Toxic workplace behavior
UIT	Unintentional insider threat
USIC	United States Intelligence Community

1 Introduction

The intelligence community needs innovation and innovation involves risk (STAR, 2020). Intrapreneurs are employees that use their entrepreneurial spirit for the benefit of their employer to produce impactful innovations (Pinchot & Soltanifar, 2021). The risks and negative spillover associated with intrapreneurial ventures and how they are perceived are not thoroughly explored in literature on intrapreneurship, although risks and non-productive outcomes have been observed (Elert & Stenkula, 2020). Despite a clear potential for overlap of the two phenomenons of intrapreneurship and insider threats, no academic literature on intrapreneurs as insider threats was found in the research for this thesis.

This Rogerian literary review answers the research question *"How can intrapreneurs be recognized as insider threats?"* The answers provided aren't all-encompassing or elaborate, but uncovers understudied perspectives from where intrapreneurs can be recognized as insider threats, and connects them in analysis for future research and further synthesis.

A range of perspectives are then cursively applied to the case of Intellipedia, as suggestions for further research rather than as rigid tests of their validity. Intellipedia – the U.S. intelligence community's digital information sharing platform, in essence its own internal Wikipedia – is used as it has been recognized both as an intrapreneurial venture (Arnold & Magia, 2013), and as an insider threat. One of the two intrapreneurs awarded for Intellipedia (CIA, 2009), Sean Dennehy, has publicly recalled how ”We were called traitors, [and were told] we were going to get people killed” (Havenstein, 2008).

2 Background

2.1 Intrapreneurs

Intrapreneurs are employees who use their entrepreneurial spirit for the benefit of their employer. Whilst supported by sponsors higher up in their organization (Pinchot & Soltanifar 2021), they also tend to evade their organizations' control systems and/or resource management to achieve their missions (Pinchot 1985, p. xi).

The term was introduced by Pinchot & Pinchot (1978) in describing ”employee entrepreneurs who work Within the corporation”. The most prevalent definition of intrapreneurs is perhaps the one from Pinchot's bestselling book (1985), describing them as "dreamers who do. Those who take responsibility for creating an innovation of any kind within an organization." In the case of Intellipedia, Sean Dennehy and Don Burke are identified as intrapreneurs (Arnold & Magia 2013).

Intrapreneurship has also been labeled as *Corporate Entrepreneurship* (Zahra 1991), *Internal Corporate Venturing* (Garud & Van de Ven 1992), *In-house entrepreneurship* (Sanghvi 1984) and *proxy-entrepreneurship* (Foss et al. 2007), although some differentiate between these and yet other, adjacent or corresponding terms (Birkinshaw 2003).

In academic literature, intrapreneurship is recognized as intra-organisational initiatives driven by employees, whether as responses to “requests and challenges from a firm's leadership” or as spontaneous bottom-up initiatives (Pinchot & Soltanifar 2021, p. 235). In both cases, intrapreneurial ventures are approved by upper management as they align with the organization's strategy.

Intrapreneurship has been linked to business growth and improvement of corporations in a Portuguese SME-context (Augusto Felício, Rodrigues & Caldeirinha 2012) and is recognized as a key driver ”underlying the competitive advantage of organizations” (Lukes & Stephan 2017). Intrapreneurship opportunities have also been linked to lower employee turnover intention (Bulmash & Winokur 2020). However, intrapreneurship has also been connected to short term risk and harm to companies (Augusto Felício, Rodrigues & Caldeirinha 2012). Also, Enron, famously dubbed ”America's most innovative company” by Fortune magazine six consecutive years, and its dramatic collapse, has been studied as a catastrophic case of intrapreneurship management, caused by ”an overabundance of entrepreneurial space” (Birkinshaw 2003).

The threats and risks associated with intrapreneurship are not well understood or explored in general, and seemingly not at all from perspectives provided by research on insider threats. As Elert & Stenkula (2020) concludes: ”Most intrapreneurship research assumes that the phenomenon is beneficial.”

However, intrapreneurial initiatives have been recognized for "working to circumvent or even sabotage the formal systems that supposedly manage innovation" and “routinely bootleg company resources or ‘steal’ company time to work on their own missions” (Pinchot 1985, p. xi).

The seemingly paradoxical approval (or encouragement) of rebellious deviance – rule breaking – from upper management might be understood as a way to circumvent or "go through the 'clay layer' of middle managers who are usually driven so hard to achieve short-term goals in established systems that they have no time for new ideas" (Pinchot & Soltanifar 2021, p. 240). To Pinchot, from a corporate management perspective, "Intrapreneuring is a more timely and effective way of conceptualizing the control task, not an abdication of control" since, "As one intrapreneur put it after a 'midnight requisition' of a major piece of capital equipment needed by his team, 'Nothing is as out of control as a large control system.'" (Pinchot 1985, p. 303). In his opening "Memo to the CEO" Pinchot concludes that "There is a revolution about to happen in your corporation. Let it start with you." (*ibid*, p. xiii).

One distinction between benevolent intrapreneurs and harmful entrepreneurial insiders is offered apropos intrapreneurial endeavours in the US military by Cambpell (2012): "While entrepreneurs define their own desired end state, intrapreneurs operate with the mission and values of their respective organization". "Entrepreneurs" are here defined as not only self-managed but with a strategic vision different from that of their organisation, whereas intrapreneurs "must be willing to accept full responsibility in the case of failure, and be equally willing to defer credit to the organization in the case of success" (*ibid*).

2.2 Insider threats

Insider threats are for this thesis defined as people who, through authorized access to an organization's resources, have the potential to negatively affect the organization, its purpose and/or its stakeholders, and that risk doing so. Several types of intentional insider acts have been identified, such as fraud, theft, terrorism, and espionage (Bell, Rogers & Pearce 2019). However, most harm from insiders is ascribed to unintentional acts: ”honest people making honest mistakes" (Pfleeger, Lawrence Pfleeger & Margulies 2015).

In academia, insider threat is an interdisciplinary subfield mainly studied from two different perspectives: computer science and intelligence studies. The two intersect as both explore questions of security and information and can, to various degrees and with varied success, build upon each other's findings. Scholars researching intelligence, counterintelligence and national security perspectives of insiders and insider threats refer to studies in cyber security (e.g. Bell, Rogers & Pearce 2019), and vice versa (e.g. Mundie, Perl & Huth 2013).

The lack of a standard definition of "insider threats" and "insiders" has been a problem in research, Mundie, Perl & Huth (2013) noted when they explored 42 different definitions of the terms[1]. Their own definition of the term ”insider threat" reads as follows:

[1] In referring to ”the" insider threat field, Mundie, Perl & Huth (2013) did not specify if that field of research pertained to intelligence, counterintelligence and national security, to cyber security or from both. The definitions that they studied did come from both types of sources. One might

> *Current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.*

This definition equates "insider threat" with "insider", as harm is already done. In contrast, others describe a threat as "a set of circumstances that has the potential to cause loss or harm" (Pfleeger, Lawrence Pfleeger & Margulies 2015, p. 5). People that have already caused harm, i.e. threats that have performed (at least some of) their harmful potential, are referred to simply as "insiders"[2] (*ibid*, p. 498) and their actions as "insider acts". Deliberate actions with the intent to cause harm are described as ”insider attacks" (*ibid*, p. 844), and their perpetrators ”malicious insiders", whilst human threats without intent to cause harm are defined as benign or non-malicious (*ibid*, p. 42). With this definition of the term, Pfleeger, Lawrence Pfleeger & Margulies identify benign insiders as the most common harmful insider in computer security: "The vast majority of harm from insiders is not malicious; it is honest people making honest mistakes" (*ibid*, p. 5). A similar term is "unintentional insider threat (UIT)", describing those "whose actions unintentionally expose the organizations to risk" (Greitzer et al. 2014), or those who ”accidentally affect the confidentiality, availability, or integrity of an organization's information or information systems, possibly by being tricked by an outsider's use of social engineering" (Cappelli et al. 2012, p. xxi).

As this thesis is published, Creech (2020), a veteran of more than 20 years in intelligence and national security, researches toxic workplace behavior (TWB) as a potent insider threat in intelligence organizations.

Following the tradition recognized by Bishop & Gates (2008), where ”each researcher develops their own definition that is particular to their own data set, situation, biases and assumptions", this thesis offers its own definition of what constitutes an insider threat:

> *Someone who, through authorized access to an organization's resources, has the potential to negatively affect the organization, its purpose and/or its stakeholders, and risk doing so.*

The last three words in this definition – addressing not the potential to cause harm but the propensity to cause harm – connects this definition to studies in motivators for (Nurse et al. 2014), identifiers of (INSA 2017), and interventions against (e.g. Bell et al. 2019) harmful and, more often than not, malicious insiders.

[2] To further complicate matters, an "insider" need not be defined as harmful in literature on intelligence, counterintelligence and national security. For example, the insiders recognized in a recent article on the US intelligence community's relationship with White House administration, are persons trusted by the president nomather what the impact of their actions or advice might be (Manjikian 2020).

2.3 Rogerian strategy

This thesis applies a Rogerian strategy as a theoretical approach, to identify and understand how intrapreneurs can be recognized as insider threats.

Rogerians seek to resolve conflict by enabling adversaries to understand one another, to empathize with each other and find common ground, seeking shared and mutual understanding and learning. By *"listening with understanding"*, one can*"see the expressed idea and attitude from the other person's point of view, to sense how it feels to him, to achieve his frame of reference in regard to the thing he is talking about."* (Rogers 2017). Building on this notion, Baumlin (1987) stated that:

> *"we fight because we have forgotten that we can change ourselves, change each other, grow towards each other rather than apart"*

Rapoport (1960) and later Young et al. (1970) contrasted Rogerian strategy against two other ways of changing people, namely the Pavlovian and the Freudian strategy:

Pavlovan strategy understands people as "a bundle of habits that can be shaped and controlled" (Rapoport 1960) through incentives and disincentives. In existing literature on innovation management and intrapreneurship, the Pavlovan strategy is often implicitly assumed, as when Elert & Stenkula (2020) concludes that *"the rules at different layers of society must be aligned in a way that results in a relative payoff structure that incentivizes fully productive intrapreneurship—at both the firm and societal level."*

Freudian strategy recognizes people as influenced by their unconscious motives, unknown to themselves. It proposes that people can change if their hidden motives are revealed. In line with Rapoport's definition of Freudian strategy, one could change persons recognizing intrapreneurs as insider threats by revealing their unknown motivations, whether they relate to ambitions, fears, or childhood traumas.

Rogerian strategy recognizes people as protective against what they perceive as threatening. It proposes that people can change if the perceived threat in changing is removed. For such threats to be substantially removed, they must first be understood and articulated. However, in contrast to Freudian strategy, articulation is not sufficient to a Rogerian: the threat must be removed. It is in line with the Rogerian strategy that this thesis attempts to articulate ways to recognize intrapreneurs as insider threats.

In lack of access to sources voicing such criticism against Intellipedia, this thesis is only equipped with the recorded statement by Dennehy that such accusations had been voiced (Havenstein 2008).

Rogerian argumentation has been criticized for its limitations (or fallibilities) in addressing structural inequities such as gender inequality (Lassner 1990) and racism (Pâquet 2019), and – in the context of nondirective psychotherapy – to hamper reflexivity amongst its practitioners (Margolin 2020). The two former share a critique about how victims rather than perpetrators are proposed to address injustices, and they all concern "underlying problems with power relations" (Pâquet, 2019) in Rogerian argumentation.

2.4 USIC’s perceived need for innovation and risk tolerance

Intelligence services are arguably always in need of innovation in order to “create an agile and successful organization able to continuously adapt its business processes to the development of society and targets” (Nicander 2011). Today, the challenges posed to intelligence services and their traditional tradecraft include the adaptation of technologies in fields such as biometrics, computer science and surveillance, the digital transformation of society in general and perhaps specifically cyber warfare (McLaughlin & Dorfman 2019).

In military technology development, the US has enjoyed a “scientific advantage upon which U.S. military dominance relies” since the end of the Cold War (Javorsek et al. 2015). This dominance might be eclipsed by China in the future, Javorsek et al. suggested. Last year, the U.S. House Permanent Select Committee on Intelligence's Subcommittee on Strategic Technologies and Advanced Research (STAR 2020) stressed the importance of innovation exploitation in the intelligence community (USIC):

> *We must act now. Studies, reports and commissions have warned for decades about the risks to national security from the steady erosion in our innovative capacity. Those risks are no longer abstract or speculative. They are upon us and presenting us with ever more adversity and ever more limited policy options.*

The report recognizes that the USICs innovative capacity is ”constrained by necessary secrecy, compartmentalization and rules”, and ”a culture that often punishes risk and cements the status quo” (STAR 2020, p. 1). The report identifies intolerance of risk as ”the most unsettling [stated problems of USIC] from the standpoint of innovation”, stating that its effect can be lethal (*ibid*, p. 10). Earlier the same year, the CIA launched a research and development initiative, ”CIA Labs”, to better address such challenges (CIA 2020).

The USIC’s different branches are not only prolific and well funded but also, in comparison with other countries' equivalents, relatively open to study and scrutiny. This makes Intellipedia, serving many intelligence services of the USIC (Lardinois 2009) a good case to examine.

2.5 Intellipedia

Intellipedia is a digital platform for collaborative, asynchronous information sharing within and between different U.S. intelligence agencies. It uses the same software as Wikipedia to implement three wikis – ”site[s] that can be modified or contributed to by users” (Encyclopædia Britannica 2018) – on different clearance levels to compartmentalize sensitive information (CIA 2009). It even had an ”import from Wikipedia”-option in an earlier version (Dennehy 2008), where analysts could easily transfer information from Wikipedia to Intellipedia. In March 2017, one of its founders (Dennehy 2017) stated that Intellipedia had received ”about 350 Million pageviews” since its inception more than ten years earlier.

Whilst the idea for the Intellipedia is attributed to the then head of the CIA’s unit for collaboration technologies, Calvin Andrus (Tomlin 2005) and his article in Intelligence Studies, “The Wiki and The Blog” (Andrus 2005), it was CIA’s Sean Dennehy and his colleague Don Burke that are credited for spearheading the initiative (CIA 2008). Tested in 2005 and announced formally in 2006, Intellipedia soon became something of a trophy project for the US Government[3]. Dennehy later recalled how ”I thought I was working for our public relations office [because] I was up in their office so often about Intellipedia” (Dennehy 2008). However, the Intellipedia project was also met by skepticism from members of the USIC (Dixon & McNamara 2008). Sean Dennehy, later publicly recalled: ”We were called traitors, [and were told] we were going to get people killed” (Havenstein 2008).

Intellipedia has been recognized as an intrapreneurial venture by consulting firm Deloitte (Arnold & Magia 2013) and has been covered in many news articles, but is generally understudied in academic literature. Intellipedia is presented as a case of one of three ”distinct legislative approaches” to increase federal counterterrorism information-sharing by the U.S. Congress, namely ”the consent approach” (Peled 2016). Similarly, a conference talk (not cited by Peled) details how the U.S. Information Sharing Environment (ISE) has benefited from Intellipedia (Willbrand 2010). Both contributions mention Intellipedia as a response to the political pressure for more information sharing within the USIC, in the wake of the 9/11 terrorist attacks against the U.S. in 2001. Other than this, Intellipedia is named in student papers, namely Eli & Hutchins (2010) and Chomik (2012)[4]. The latter student also wrote an article mentioning Intellipedia published in a journal the year before he presented his master thesis (Chomik 2011). Also, there is an ethnographic study made by the Defense Intelligence Agency’s (DIA) Knowledge Lab, of how DIA analysts use and experience the Intellipedia, independently published online by one of the researchers (Dixon & McNamara 2008). This DIA study is made from unclassified data extracted from interviews (with ten analysts identified as active users of Intellipedia and five identified as non-users), all anonymized. The researchers stated reluctance to call their results ”finding” and instead presented them as observations, as there was no systematic sample of respondents and because the sample size was relatively small (this study is one of two main sources used by Chomik 2012).

[3] e.g. promotional recruitment video ”Intellipedia” (USAJOBS, 2013) & the Service to America Medal awarded to its two ambassadors (CIA, 2009)

[4] The author found one more academic product that might have used Intellipedia as a case, but as it was anonymized in exchange for greater access, it won’t be mentioned here.

3 Methodology

Analysis of the empirical base – the literature surveyed for this thesis – is conducted through thematic text analysis: searching for fruitful analogies, dominant themes, similarities and differences, and theory-related material in line with Ryan and Bernard (2003, p. 90-93), as cited by Bryman (2012, p. 580). Referenced audio and video recordings have been transcripted with an automated transcription service[5], manually edited for legibility and time coded by the author, and then (as other data) coded for analysis.

This thesis is a narrative literature review (NR) of perspectives to understanding how intrapreneurs can be recognized as insider threats. As NRs are criticised for subjectivity in study selection (Ferrari 2015, p. 231), and reviews ”are written from a particular perspective or standpoint of the reviewer” (Hart 1998, p. 25), author's experiences and bias is explained in this chapter.

3.1 The rhizomatic snowball fight

Rather than snowball sampling, where a small sample of literature relevant to the research question is chosen as a starting point, and other literature is then proposed through that literature, via citations (to) and references (from) key literature – as described by Bryman for human respondents rather than articles (2012, p. 424) – this thesis research design could be described as ”snowball fight sampling” where several entry points into literature have been explored simultaneously and in concert. ”Snowballs” have fusioned and fissioned as they've been non-hierarchically and asynchronously connected and separated in analysis. The author has, in no particular order but often in symbiosis:

- drawn from his own pre-existing theoretical and tacit knowledge,
- jumped into innumerable rabbit holes of literature (academic and popular),
- consulted scholars and practitioners alike via email, Linkedin messaging, and phone to ”enter into dialogue with [them] as a way of determining shared and and nonshared images, beliefs, and values” (Bator, 1992, p. 86), in line with Rogerian strategy – and in search for greater credibility.
  - **Gifford Pinchot III** (co-creator of the term intrapreneurship),
  - **Matt LeMay** (author, management consultant and critic of rule-breaking), and
  - **Jan Goldman** (editor in chief of International Journal of Intelligence and Counterintelligence) all deserve special credit for their helpful correspondence.
- brainstormed hypotheses around intrapreneurship as insider threats,

[5] The machine learning service ”IBM Watson Speech to Text” is available through a demo-site.

- browsed through indexes of relevant journals in search for more leads,
- Published drafts for this thesis on a blog created for this purpose, garnering some 200 visits and 300 pageviews, but relevant feedback in comments or emails.

To some extent, this can be described as a rhizomatic approach as it ”moves in many directions and create[s] a multiplicity of connections and relations” (Movahedian et al. 2020). But whereas Deleuze & Guattari (1987, p. 9) states that *”There are no points or positions in a rhizome, such as those found in a structure, in tree or root”*, the literature presented in this thesis have been structured for legibility.

It’s easy enough to study the literature referenced in this thesis, scrutinize the interpretations and test the suggested connections. However, the rhizomatic snowball fight sampling is impossible to replicate or validate. The author recognizes this as a flaw in the research design, guilty of the critique around replication issues in qualitative research (Bryman 2012, p. 405), but finds that this ‘good enough’ approach nevertheless gets the job done: relevant and previously undocumented connections in literature have been uncovered.

Some concepts and theories have been excluded after more rigorous review and analysis than others. Literature on platformization – the drive towards ”the platform as the dominant infrastructural and economic model” (Helmond 2015) – and the adjacent concept of Government as a Platform (GaaP) – ”platforms deployed to coordinate and control service productions in the different domains of government intervention” (Cordella & Paletti, 2019) – being the most notable example. The available research into it was deemed too nascent to apply to this thesis’ research question, even though
1) intrapreneurial efforts can be facilitated or even mandated through platformization[6].
2) platformization might soon influence intelligence services much more, and
3) Intellipedia is a platform deployed to coordinate service production in the USIC.

3.2 Critical Realist Grounded Theory

Collection and assessment of applicable literature have been conducted simultaneously in line with Oliver’s (2012) suggestion for Critical Realist Grounded Theory (CRGT), spanning traditional divides between positivist, post-positivist, constructivist and critical philosophical paradigms (*ibid*, p. 372):

> *”It marries the positivist’s search for evidence of a reality external to human consciousness with the insistence that all meaning to be made of that reality is socially constructed.”*

As CRGT ”accommodates researchers’ pre-existing theoretical knowledge, hunches and hypotheses as necessary ‘points of departure’ [...]”, a brief account of author’s experiences and bias is included in this thesis.

However, CRGT is not practiced orthodoxically for this thesis. Retroduction – ”abduction with a specific question in mind” and ”the central tool of critical realist

[6] e.g. Chinese firm Haier and it’s management philosophy ”Rendanheyi 2.0”, where the company has transformed into a conglomerate of – or a platform for – micro-enterprises (Hamel & Zaninini 2018), and similar constructs like Kollmorgen’s independent product lines described by Pinchot (1985)

inquiry” (*ibid*, p. 379) – has not been applied *in extenso*. Although questions like ”what must be true for this to be the case?” and ”what makes this possible?” have been asked of the material, explanations of ”generative mechanisms at a deeper ontological level” have not been sought to the fullest and are even less so detailed in this thesis.

3.3 Limits of Rogerian approach

To attempt a Rogerian approach when at least one central part of the conflict is missing, and instead search for arguments to support its position – recognizing intrapreneurs as insider threats – in academic literature, is admittedly a bold enterprise. To achieve meaningful understanding of the perspectives of these critics, in-depth interviews and/or participatory observation would be more appropriate methods than a literary review. Nevertheless, as the perspectives of critics and sceptics cannot be attained within the scope of this thesis, a Rogerian literature review is a second best: Rather than understanding – *verstehen* (Weber 1904) – the points of view of these skeptics or critics of intrapreneurial ventures, this thesis explores perspectives where intrapreneurs can be recognized as insider threats through existing literature.

If “theories are stories” (Goodson, 2010), Rogerian argumentation can easily end up reinforcing the stories of the powers that be, even if they ought to be challenged, according to critics like Lassner (1990), Pâquet (2019) and Margolin (2020). In searching for possible perspectives on how intrapreneurs can be recognized as insider threats, this thesis has focused on perspectives beyond what Allison (1971) would call "governmental politics". However, perspectives beyond that of the rational actor-perspective (e.g. critical studies of how leaders might exploit intrapreneurial concepts to reaffirm their dominance by letting loyal junior members “rebel” against more senior contestants for power, or of organizational incumbents that label intrapreneurial challengers for power as insider threats to secure their own standing in the organization) might be very relevant.

An unreflective Rogerian approach would be to not admit this limitation in scope and reasoning. Although this thesis explores perspectives supporting critics and sceptics to intrapreneurial ventures through a ”Model I”-perspective of participants as rational actors (Allison 1971), other perspectives also apply for insider threats and intrapreneurship, and their critics, alike.

3.4 Aiming for ”That’s Interesting!”

Stating that this thesis’ research question was formulated purely out of Rogerian ambitions would be false. It is also inspired by Davis’ (1971, p. 311) assertion that ”All interesting theories [...] constitute an attack on the taken-for-granted world of their audience.” Although this thesis does not attempt to forge new theory, it does try to be interesting. As Elert & Stenkula (2020) asserts, the relatively rich literature on intrapreneurship features little research on the destructive potential in intrapreneurship.

Predicting an audience for a bachelor's thesis is a vain affair, but let's entertain the notion that someone, somewhere, reads this:

1. As scholars generally conclude or assume that intrapreneurs are beneficial to organizations, suggesting that they can be insider threats might make someone ”sit up and take notice” (Davis 1971, p. 310).
2. As many intrapreneurs – in the author's lived experience, according to the correspondence with practitioners for this thesis, and in Pinchot's literature (e.g. 1985) – dismiss antagonists within their organizations as ignorant if not malicious, proposing a Rogerian approach to understand perspectives from where an intrapreneur is recognized as an insider threat might not only appear as an interesting theoretical proposition, but inspire practical implications.

These two imagined audiences – researchers and intrapreneurs – are thus presented with one proposition each that negates their accepted presumptions (Davis 1971, p. 313).

One could argue that the context wherein an intrapreneur is or might be recognized as an insider threat is important to assess the relevance in perspectives in literature. That is true. However, apart from the scope of this thesis, Healy's (2017) arguments against nuance has helped in avoiding such distinctions. The findings in this thesis wouldn't be any more intellectually interesting, nor empirically generative or practically successful if more context than the illustrative case of the USIC and Intellipedia was considered.

3.5 Author's experience and bias

This study of intrapreneurs as insider threats is inspired by the author's lived experience as a business developer in a multi-national news corporation's “innovation hub”, or new ventures unit (NVU), as well as more than a decade's prior experiences with corporate innovation and entrepreneurship. The author found the power dynamics, resource management, and interpersonal interactions involved much more fascinating and multifaceted than what a cursory review of business and academic literature revealed.

The author has no experience of intelligence services, let alone in the USIC or with Intellipedia. This inhibits the level of insight and understanding, especially given the secretive nature of the institutions involved.

One of the teachers of this thesis course, possibly the one who will grade it, has inadvertently inspired this thesis with his article on the Nordbat 2 mission in Bosnia (Ingesson, 2017).

In addition to gratitude for his time, Pinchot's persona and credentials might have affected the author's judgement in interpreting his work.

The author's personal position, at the start of this research, was that innovation and development – and thus at least some sort of intrapreneuring – are integral and inevitable parts of organizational life, as organizations and the circumstances under which they operate are ever changing. The author also regards risk as inevitable, as per Schumpeter's (1942) gales of creative destruction, and was surprised to find so little research on the destructive potential of intrapreneurship.

4 Material

In line with the tradition in intelligence studies ”characterized by its inter-disciplinary character and openness to different conceptual approaches" (Scott & Jackson 2004, p. 139), literature from a range of different disciplines and fields have been explored: economics, computer science, intelligence studies, law, and political science. They fit in a (very) wide-tent definition of organizational theory. Although material from the disciplines of psychology and ethics (and other disciplines of philosophy) are most likely relevant, they have only been explored in the instances where they were incorporated into the research by the literature presented in the Findings chapter below. This selection was made to make the scope of research manageable.

This thesis does not study the actual skeptics and critics of Intellipedia or their arguments and positions. Finding such critics and receiving high enough clearance and trust to have them speak candidly about their concerns was deemed beyond the scope of this thesis. Also, the concerns relayed in secondary and tertiary sources (e.g. Dixon & McNamara 2008 and Havenstein 2008) was deemed too poor as data to consider for analysis. Instead, this thesis seeks arguments for recognizing intrapreneurs as insider threats in the aforementioned range of academic literature.

The complementary material on the USIC and Intellipedia is primary sources in forms of presentations and press releases, and secondary sources in forms of promotional videos, interviews, articles and presentations.

Pinchot’s ”Intrapreneuring” (1985) is referenced throughout this thesis. It is, even by business literature standards, written in a very unapologetic inspirational tone. The role of the intrapreneur is problematized only superficially, as are objections against intrapreneurship. The book is not academic literature, but has inspired hundreds of academic articles and is mentioned by most. Its arguably quite one-sided, positive perspective of the intrapreneur also echoes in much academic literature.

5 Findings

In reviewing different perspectives in existing literature and tentatively assessing their applicability in understanding how intrapreneurs are recognized as insider threats, three core themes emerged, more or less corresponding with other, existing fields of research. The three themes, presented below, are ”Threatening resources”, ”the fight for trust”, and ”Threatening transformation”.

5.1 Threatening resources

Under this theme, both threats of depleting scarce resources and threats of potentially harmful use of resources are considered and explored. Resources are defined as all assets, capabilities, processes, attributes, information, knowledge, etc. controlled by the organization that enables it to conceive of and implement strategies that improve its efficiency and effectiveness (Barney 1991, p. 101, referencing Daft 1983). Moreover, the general categorization of organizational resources in material, human, financial, and information resources is used to differentiate between different types of resources.

In applying a lens of ambidextrous organizations, conflicts around resources are limited to those between exploitation (i.e. streamlining resources for maximal output and minimal risk) and exploration (i.e. innovation involving risk and redundancy).

By exploring perspectives on secrecy vs. openness, it is recognized that the conflicts around resources are not limited to scarce resources. As implied in this thesis’ definition of insider threats, conflicts can also arise around the potential harm in (or devaluation of) informational resources that are not scarce by nature but by design, namely through classification and compartmentalization.

By exploring conflict over human resources, their tendency to be both scarce and risky is recognized. With risk of stating the obvious: careless or malicious employment of human resources is the root cause of insider threats being realized, at least from a managerial perspective.

In the case of Intellipedia, conflict over scarcity primarily applies to human resources. Conflicts over risks involved in employing resources, however, applies to both to information resources and human resources.

5.1.1 Ambidextrous organizations

Since the early 1990s, one popular approach to study and describe the balance between innovation and efficiency within organizations has been the notion of ”Ambidextrous organizations”: where exploration is handled with one hand and exploitation with the other, prompted by the observation by March (1991) that *”Both exploration and exploitation are essential for organizations, but they compete for scarce resources”*.

More recently, Magnusson, Koutsikouria & Päivärinta (2020) found in studying IT governance in the Swedish Tax Authority a *”substantial misalignment of the tactical vs. the strategic and operative layers”*. Whereas the strategic intent and the actual outcome aligned fairly well, project goals set by middle management all but eradicated exploration in favour of exploitation.

The authors explained this as *enactment* (rather than management or design) of ambidextrous IT Governance, where ”efficiency creep” in the middle layer is balanced by ”shadow innovation” in the bottom layer in the organization’s hierarchy. Shadow innovation is defined as involving unsanctioned activities, fitting Pinchot’s (1985) description of intrapreneurs who “routinely bootleg company resources or ‘steal’ company time to work on their own missions”.

Magnusson’s et al.’s findings could indicate that there’s not only demand for exploratory intent to ”go through the ‘clay layer’ of middle managers who are usually driven so hard to achieve short-term goals in established systems that they have no time for new ideas”, as Pinchot & Soltanifar (2021) suggest, but that – through enactment of ambidexterity – can be accomplished.

5.1.2 Information - more risky than scarce

Informational resources, that in a digital context can be infinitely and instantly copied and distributed, are not bounded by scarcity, but to 1) reduce risk and 2) increase advantages. Both reasons can be found in Shulsky & Schmitt’s (2002, p. 172) thoughts on intelligence and secrets: ”Fundamentally, intelligence seeks access to information some other party is trying to deny.” and, consequently, ”One side’s intelligence failure is likely to be another side’s counterintelligence success.” This logic makes open source intelligence a second best: ”open-source is primarily a means to get around the barriers that obstruct direct access to the information being sought”. Perhaps consequently, Pedersen & Jansen (2019) found that intelligence analysts labeled secret intelligence as more credible than identical open-source intelligence, when addressing complex problems with high uncertainty.

In the case of Intellipedia, Sean Dennehy (2008, 58:40) recounts how members of one organization with access to the platform demanded that data on the ”top secret network”[7] be deleted, as it was ”’compartmented information’”. Dennehy and his colleagues quickly realised that the information in question was in fact imported verbatim from Wikipedia, the web encyclopedia. This did not satisfy the people demanding a redaction: ”they were like ‘NO, no it doesn't matter, you still need to take it down’”. This anecdote illustrates the overzealous compartmentalization that Intellipedia was meant to help remedy (Willbrand 2010 & Peled 2016). Unfortunately, it doesn’t explain *why* the contacting organization wanted the information removed. A better understanding of their motivations

[7] This is presumably the secure intranet system JWICS, where the most secret of the three wikis that constitute Intellipedia resides.

might aid to alleviate their problems, rather than try to eradicate the consequences/symptoms (e.g. over-compartmentalization) of those problems.

Javorsek et al. (2017) identifies four major victims of ”over-compartmentalization” of knowledge in an intelligence context: intelligence products, efficiency, intellectual ability, and information sharing between the tactical and strategic level. Quoting Kitrosser (2008), they do recognize that ”security compartmentalization has both costs and associated benefits". However, the candor argument brought forward by Kitrosser – that secrecy can further openness since *”candor may more likely emerge in a closed, confidential conversation than in a public one”* – is seemingly ignored by Javorsek et al. when they conclude that compartmentalization equals *”increasing costs in research and development”.* It’s perhaps worth noting that Kitrosser’s article addresses congressional oversight of national security activities and not intra-organzational development per se. One might assume that Javorsek et al. considers the candor-argument less applicable to technological R&D than intelligence analysis and intelligence operations, the fact that increased psychological safety affects team learning behavior (Edmondson 1999) aside. Kitrosser also concludes that ”The purpose and utility of funneling have been under-explored, and funneling's propriety and implications thus are poorly understood.”

5.1.3 Human resources – scarce and risky

One key resource handled by ambidextrous organisations is human resources (Magnusson et al. 2020, p. 13). A perceived example of conflict over employees’ scarce amount of time and attention are also recounted in presentations by Intellipedia’s intrapreneurs (Dennehy 2008, 01:12:15). However, conflict over human resources needn’t arise from them being scarce. They can also cause harm, especially if employed carelessly or maliciously in a national security context, whether by toxic or workplace behaviour (Creech 2020, p. 9) or other destructive deviance directed towards individuals, or by property or production deviance harming the organization and its purpose (INSA 2017, p. 5)

In a rare study of a specific type of negative spillover from intrapreneurial activities, Eyal-Cohen (2019) identified the risk of losing intrapreneurial talent and intellectual property (i.e. human and informational resources) either to incumbent competitors or new ventures, and repressive and/or wasteful arrangements to mitigate such risks, as potential negative spillovers of intrapreneurial firms. As mentioned earlier Eyal-Cohen’s article was followed by (but not mentioned in) research linking intrapreneurship opportunities to lower employee turnover intention (Bulmash & Winokur 2020). In an intelligence context, the incumbent competitors aren’t only found in the domestic private and public sector, but could of course also reside in a hostile foreign state.

5.2 Trust issues

Positive expectations – trust – in organizations, whether residing with the public, with other external stakeholders, or within the organization, can be regarded as a resource (e.g. Zand 1997, Davis et al. 2000, and Dirks & Ferrin 2001). However, as this question is central to the question of how intrapreneurs can be recognized as insider threats, and several promising perspectives have been found, it has been designated its own core theme, rather than sorted under ”Threatening resources”.

The importance of trust/distrust – and the ambiguous nature of the term trust – was recently acknowledged and scrutinized by Manjikian (2020), investigating trust relationships between the USIC and its US presidents over the years. She concludes that questions about trust are complicated by the term’s ambiguity: ”Trust can be understood as a psychological state, as a measure or competence or reliability, or as a strategic interaction” (*ibid*, p. 727). In the following analysis, both understandings are considered.

5.2.1 The balance between personal vs. organizational risk

Intrapreneurship is often pitched to employees ”as a way to capture the creativity and excitement of entrepreneurship, albeit with more resources and less risk” (Pinchot & Soltanifar 2021). However, the first principle of eight in the whitepaper introducing the term is ”*To become an intrapreneur, an individual must risk something of value to himself*” (Pinchot & Pinchot 1978)

In exploring ”a paradoxical nature of translation of individual level risk aversion into organizational level risk taking behavior”, Antoncic (2003) used several perspectives to understand and explain relations between intrapreneurship and risk, namely four ”congruent and complementary" theories around information processing:

- The Theory of Planned Behaviour (where decisions are considered to be based on salient beliefs),
- Prospect Theory (where decisions are considered to be based on perceptions of information),
- Agency Theory (where decisions are considered to be based on information availability related to financial relationships in their organizations) and an
- Organizational Culture Perspective (where decisions are considered to be based on information availability related to non-financial relationships in their organizations).

In his research, Antoncic found that the paradox he explored didn’t tend to impact context specific risk-related cognitions and behavior. He offered the ”radical conclusion” that it doesn’t exist, and the ”more moderate explanation, which seems to be more plausible” that it doesn’t harm or disturb organizational life and performance. Regardless of whether or not his proposed paradox exists or not, his investigation of intrapreneurial risk taking and set of theories to explain it might serve further investigation into how intrapreneurs can be recognized as insider threats well. After all, intrapreneurs are not necessarily less threatening if their individual level risk aversion is as low as their propensity for organizational level risk is high.

5.2.2 Evasive entrepreneurship

This evolving field of research study companies' relations to societies. Elert and Henrekson (2016) defines evasive entrepreneurship as ”profit-driven business activity in the market aimed at circumventing the existing institutional framework by using innovations to exploit contradictions in that framework”. Exploitation can be enabled by regulatory vacuum, vagueness or incompetence. Elert & Henrekson states that while evasive entrepreneurship can be either productive, unproductive or destructive, it can also challenge the status quo through disruption. To understand how intrapreneurship can be recognized as an insider threat, a tentative translation to evasive intrapreneurship could be made. The ‘midnight requisition’ described by Pinchot (1985, p. 303) might be described as such, and recognized as an insider attack.

The most explicit description of evasive behavior found in presentations of Intellipedia is the recollection of how the two intrapreneurs exploited the fact that they belonged to different parts of the CIA. ”It was really helpful [...] we often used [...] both of our management chains against each other” (Dennehy 2017, 04:59).

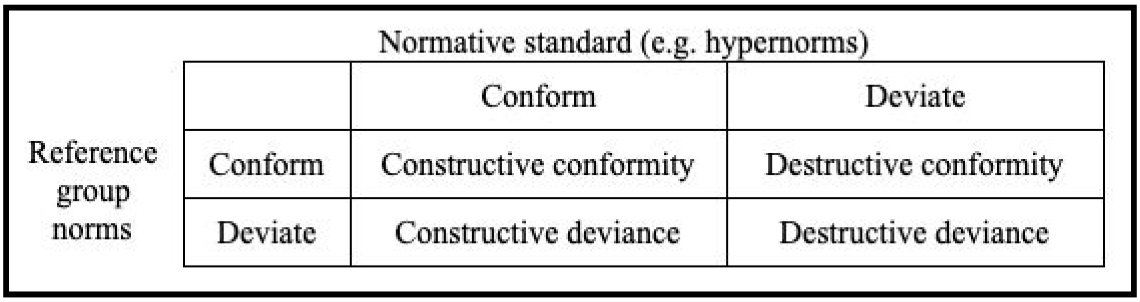
Just as evasive entrepreneurship can offer the shortest – or only – way to success in a cumbersome societal environment, evasive measures might be the easiest – or only – available option for intrapreneurs to achieve their goals.

5.2.3 Employee or workplace deviance in organizations

Warren (2003) defines employee deviance as "behavioral departures from norms of a reference group" and notes that it can cause "disastrous consequences for not only organizations but also entire industries and society”, as well as bring about constructive change and help evade organizational failure or societal disaster. To differentiate between departures from a reference group (e.g. the USIC) and normative standards (e.g. human rights), she proposed a four field matrix[8]:

[8] *Destructive conformity* should not be confused with *malicious compliance* (not mentioned by Warren). The latter describes employees carrying out orders with the knowledge and/or intent that the consequences from their compliance will cause harm to their employer. Destructive conformity might serve the organization perfectly well, but it deviates from hypernorms (e.g. human rights violations by the CIA).

figure 1. ”Typology of Employee Deviance” as replicated from Warren (2003, p. 629)



		Normative standard (e.g. hypernorms)	
		Conform	Deviate
Reference group norms	Conform	Constructive conformity	Destructive conformity
	Deviate	Constructive deviance	Destructive deviance

Judging if deviance is destructive or constructive (or simply unproductive) requires a clear and detailed position, Warren argues in one of her appeals for advancements in research. For example: simply saying that *illegal* behavior is to be deemed destructive overlooks the complexity in firms that operate in many and sometimes conflicting legislations (the same can of course be said for most intelligence services). The argument that *societal values* should define what constitutes constructive deviance or not faces the same problem: what society’s norms and values should define this? And how are those values agreed upon in the first place? Warren suggests hypernorms, i.e. ”globally held beliefs and values” to assess deviance. In contrast to ”universal norms”, where a person or a group decides what the rest of the world should agree on, hypernorms could be explained as the ”least common denominators” of what all people want and need: food, freedom, and physical security for example.

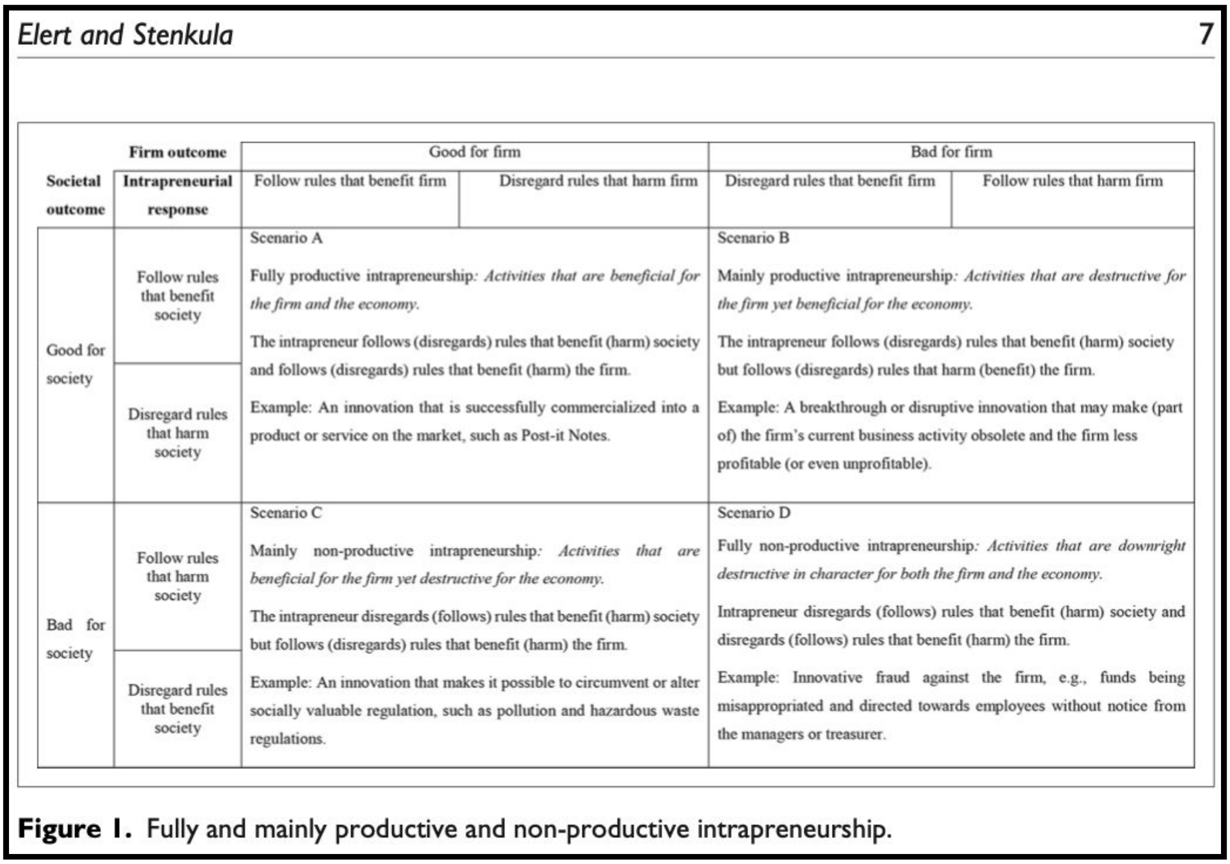
> *In essence, these metanorms provide a global standard for evaluating behavior that extends beyond organizational and country-specific boundaries. The appeal of using hypernorms as a standard for judging workplace deviance lies in their inclusiveness and ease of empirical application.*

The perspective of employee deviance is highly relevant to intrapreneurship studies in general, and especially for research into the duality of destructive and constructive deviance in intrapreneurship. Although some connections have been made between intrapreneurship and workplace deviance (e.g. Galperin 2012, Galperin & Burke 2006, Voon, Othman & Leng 2019) on one hand and workplace deviance and insider threats on the other (e.g. Green 2014, Kennedy & David 2018), no prior connection seems to exist between the three fields.

In exploring productive and non-productive intrapreneurship (where the latter includes destructive intrapreneurship), Elert & Stenkula (2020) recalls Baumol’s observation (in turn building on Schumpeter 1942) that flawed rules of the game in societies can result in entrepreneurs leading “a parasitical existence that is actually damaging to the economy” (Baumol 1990) in line with evasive entrepreneurship (Elert & Henrekson 2016). As they ”draw the corresponding implications for intrapreneurship” they recognize that Foss et al. (2007) are among the few that have done so before.

Elert & Stenkula (2020) don’t mention workplace or employee deviance, but their four field matrix bears striking resemblance to Warren’s (2003), albeit with added detail:

figure 2: Screenshot from Elert and Stenkula (2020):



Elert and Stenkula 7

	Firm outcome	Good for firm		Bad for firm	
Societal outcome	**Intrapreneurial response**	Follow rules that benefit firm	Disregard rules that harm firm	Disregard rules that benefit firm	Follow rules that harm firm
Good for society	Follow rules that benefit society	Scenario A Fully productive intrapreneurship*: Activities that are beneficial for the firm and the economy.* The intrapreneur follows (disregards) rules that benefit (harm) society and follows (disregards) rules that benefit (harm) the firm. Example: An innovation that is successfully commercialized into a product or service on the market, such as Post-it Notes.		Scenario B Mainly productive intrapreneurship*: Activities that are destructive for the firm yet beneficial for the economy.* The intrapreneur follows (disregards) rules that benefit (harm) society but follows (disregards) rules that harm (benefit) the firm. Example: A breakthrough or disruptive innovation that may make (part of) the firm’s current business activity obsolete and the firm less profitable (or even unprofitable).	
	Disregard rules that harm society				
Bad for society	Follow rules that harm society	Scenario C Mainly non-productive intrapreneurship*: Activities that are beneficial for the firm yet destructive for the economy.* The intrapreneur disregards (follows) rules that benefit (harm) society but follows (disregards) rules that benefit (harm) the firm. Example: An innovation that makes it possible to circumvent or alter socially valuable regulation, such as pollution and hazardous waste regulations.		Scenario D Fully non-productive intrapreneurship*: Activities that are downright destructive in character for both the firm and the economy.* Intrapreneur disregards (follows) rules that benefit (harm) society and disregards (follows) rules that benefit (harm) the firm. Example: Innovative fraud against the firm, e.g., funds being misappropriated and directed towards employees without notice from the managers or treasurer.	
	Disregard rules that benefit society				

Figure 1. Fully and mainly productive and non-productive intrapreneurship.

This thesis includes those who have the potential to negatively affect the organization’s stakeholders in its definition of insider threats. Therefore, ”Scenario Cs” – Warren’s (2003) destructive conformity – where intrapreneurs benefit their organization but harm society (including stakeholders) can also be recognized as insider threats. One reason for this is that societal harm will likely, eventually, hurt the organization. However, intrapreneurs adhering to an organization’s rules and norms but threatening or hurting society might not be the first to be recognized as insider threats. Intrapreneurs in ”Scenario B” and ”D” (Warren’s destructive and constructive deviance) are the most likely candidates.

In all instances of deviance, "behavioral departures from norms of a reference group", trust is threatened and/or eroded. Regardless of material or financial consequences or risks, perceived breaches of trust might be enough for intrapreneurs to be recognized as insider threats.

5.2.4 Ethics of espionage

In trying to do the right things regarding intrapreneurship, most conscientious people will run into ethical dilemmas. The examples given by Warren (2003) highlights that these questions can be particularly hairy in organizations operating in different or vague jurisdictions, like intelligence services for example.

Pfaff & Tiel (2004) tried to help intelligence professionals determine ”when it is appropriate to set aside the usual prohibitions in order to achieve national objectives”. They provided a framework inspired by Kant & Locke to find a balance between ”ethical restraint and intelligence effectiveness”.

They concluded that modern liberal republics are built on the grounds that all persons are created equal, and that acting against this principle ”would be an act of betrayal”. They added that although this should constrain the actions of intelligence professionals, they don’t have the same obligations to citizens of other nations as they do to citizens of their own. In seeking what Warren (2003) would call hypernorms, Pfaff & Tiel (2004) agree that two salient features appear to be critical to human value:

1. Metaphysical freedom: Humans can reflect upon and decide their actions independently.

2. Rationality. Humans can recognize that they are humans among humans, and that we share our freedom for choosing with the other persons we identify as humans.

From this follows the Golden Rule, similar to what Kantians refer to as *Categorical Imperative* and Lockeans call *Natural Rights*.

Pfaff & Tiell goes on to argue that, in line with the hypernorms (Warren 2003), it is ethical to respect humans accordingly ”unless they consent to be constrained by something in addition to these boundaries”. They motivate this with an obligation to respect other humans’ right to choose for themselves. This logic justifies killing a soldier in the battlefield, as that person ”accepts the training and equipment of a soldier” and thus not only poses a threat but is ”a player in the game of war” (Pfaff & Tiel 2004, p. 5).

Recognizing that people can participate more or less willingly to different degrees in a spy game, Pfaff & Tiell then goes on to sort actors in five categories of ”legitimate targets of espionage” – from the ordinary, uninformed citizen to the informed intelligence professional – specifying what different actions can be justified taking against the different categories of ”players” in spy game, and why.

The authors recognize the problem of collateral damage: ”intelligence operations directed against legitimate targets might have nonconsensual consequences for illegitimate targets”. Their solution to this problem is the doctrine of double effect, attributed to Christopher (1994) that there is ”a moral difference between the consequences of our actions that we intend and those we do not intend, but still foresee”, and that it is permissible to do something good that (also) have bad consequences, given that four conditions are met:

1. Nastiness is not intended,
2. Nastiness is proportional to the good effect’s worth,
3. Nastiness is not a direct means to the good effect and,
4. Nasty effects are mitigated, even at more high-risk expenses.

The doctrine of double effect could help in assessing intrapreneurial transgressions, such as unsanctioned risk taking, midnight resource allocation, or other evasive innovation activities. It also relates to the concepts of *acceptable loss* and *acceptable risk* (Fischhoff et al. 1984). The doctrine of double effect might also give perfectly well-intentioned intrapreneurs reason to – knowingly and deliberately – cause harm.

Ethical deliberations and frameworks are relevant to understanding how intrapreneurs can be recognized as insider threats. However, by proposing further research in this direction, this study does not suggest that official or popular judgement on intrapreneurial transgressions are made solely on moral grounds.

5.2.5 Sub-cultures on the tactical/operative level

Ingesson (2016) argues that decisions of lower-level military commanders can have ”major political and strategic impact”, and that these decisions are shaped by ”tactical-level subcultures”. He suggests that military leaders on the tactical level are in fact ”street-level bureaucrats”. This term was coined by Lipsky (1980), describing ”a public service worker who interacts directly with citizens in the course of his or her job” and through their ”substantial discretion in the execution” and relative autonomy from organizational authority can ”make policy”[9].

Because decision-making in war (fighting hostile, life-threatening adversaries with limited information, scarce time to decide and other inadequate resources – and with ”an infinity of petty circumstances” (Clausewitz 1832) adding friction) is stressful and ”extraordinary difficult” military street-level bureaucrats lean on subcultures, Ingesson argues (2016, p. 26): ”A tactical-level subculture is, in essence, a set of cultural norms, ideas and priorities, which are shared by the members of a military unit.” In his proposition lies the argument that military organizations aren’t homogenous, but ”comprised of numerous *esprits de corps*, that are constantly being reproduced within their respective units” (Ingesson 2016, p. 30-31).

An effective tactical-level subculture is coherent (i.e. straightforward and without inherent contradictions) and agreed upon by its members. This is achieved through focal points, such as a role model or tradition: ”When the members of a unit become confused as to how they should act, the focal point provides clarity” (*Ibid*)

As one example, Ingesson details how Swedish troops in Bosnia, 1993, had a ”a strong heritage of formalized autonomy” (2016, p. 237), citing their tactical manual: “Indecisiveness and lack of action usually has more severe implications than if a commander makes a mistake regarding how to proceed” (AR2 1982, as quoted by Ingesson). This helped build a ”Trigger-Happy, Autonomous, and Disobedient” (Ingesson, 2017) tactical-level subculture that in turn helped save civilian lives in spite of complicated and complicating rules of engagement.

[9] If Lipsky’s description of autonomous, almost defiant, professionals rings a bell, it’s worth noting that both he and Pinchot (1985) are men of the US “lucky few”-generation, and wrote their seminal books around the same time, in their late thirties/early forties (Lipsky was born in 1940, and Pinchot in 1942).

Although intrapreneurship is routinely described as a individual activity, cultural factors are studied (e.g. Yun et al. 2020, Hashmi & Siddiqui 2020, and Benitez-Amado et al. 2010), and although most intrapreneurs fortunately aren't exposed to the atrocities and fog of war, other uncertainties (Höyssä & Hyysalo 2009) and stressors might apply.

In the case of Intellipedia, one can speculate over why two officers from the CIA were selected to spearhead a platform serving the entire USIC, established and hosted by the Intelink office under Director of National Intelligence, DNI (CIA 2008). One possibility is that CIA's subcultures were deemed the most appropriate to lead this venture, a more likely hypothesis is that Dennehy, who was first approached (Dennehy 2008), was selected because he showed interest. Also, ”the man with the plan”, Calvin Andrus (2005), was head of CIA's unit for collaboration technologies. Yet another possible explanation is that the CIA had resources (beyond its subcultures) deemed necessary for the mission. Nevertheless, it would be interesting to learn more about how the different subcultures in the USIC interact in and around Intellipedia. A starting point could be to compare the CIA narrative with Dixon & McNamara's (2008) study on DIA employee's experience with Intellipedia. Also Chris Rasmussen, ”Intellipedian” with the NGA mentioned by Dennehy (e.g. 2008, 15:40, 18:45 & 54:15) and in news reporting (Lardinois 2009), could be an interesting data point of reference. Friction and/or misalignment between different subcultures could cause trust issues and intrapreneurs to be recognized as insider threats..

5.3 Threatening transformation

Hinings et al. (2018) recognizes that digital transformation – ”the combined effects of several digital innovations bringing about novel actors (and actor constellations), structures, practices, values, and beliefs” – can threaten the existing ”rules of the game” in and for organizations. However, they also question the idea of total disruption, and suggest that existing literature on institutional change rather suggests that if and how new arrangements are accepted depend on already existing institutional arrangements.

Hinings et al., in citing Bitektine (2011) and Suchman (1995) among others, recognizes that both accommodation marketplace Airbnb and crowdsourcing platform GalaxyZoo (now Zoouniverse) were accepted by existing institutions because they were developed and promoted ”using language that aligned them with […] organizations/industries that already had legitimacy” (Hinings et al. 2018). They propose that radical digital transformers, to be successful, seek legitimacy through and in the institutions that they challenge, often by imitating them to some extent.

Intellipedia, as a digital information-sharing tool, was recognized for its potential to transform the intelligence community (Willbrand 2010, Peled 2016, Andrus 2005, Dennehy 2008).

Sean Dennehy (2008, 34:40) mentions how one analyst (stationed in the U.S.) published a list of leaders in southern Iraq as ”red links”[10] on Intellipedia. He did it as a personal note, a ”laundry list”, of people he would like to make sense of in the future. In the following weeks, however, he found that link after link on his list turned blue, as they were filled with information by someone else:

> *”It turns out, someone in the field came across this page, saw all the red links and said ‘ah, I got someone who can report on that [...] let me go get some information for him’.”*

This example was given to illustrate that people are most likely to try and succeed in adopting new collaborative technology and practices if they are first acting for and by themselves, and then discover how their interests and contributions can add to, and be complemented by, others’ work. However, it also demonstrates the transformative power of a digital platform that undercuts established channels and lines of command.

In contrast, Dennehy’s colleague Don Burke, describes their internal framing of Intellipedia in an non-transformative fashion (USAJOBS 2013, 1:23):

> *”Our challenge throughout has been to identify and articulate how this tool can allow people to do largely the same thing that they are already doing, but in a more effective way.”*

This is one of three ”core principles” in the intrapreneurs’ strategy (Howard 2010, 05:25): to focus on replacing existing processes. It is unclear whether Burke is unaware of Intellipedia’s transformative potential, if he doesn’t make the connection here, or if he tries to gain legitimacy by stressing the likeness to standard procedures by stressing *”largely the same thing”* (something Hinings et al., 2018, might categorize as imitation). The context of Burke’s statement is a promotional video for recruiting people to government positions, not an informational video for internal use.

In his questionnaire ”*Are You an Intrapreneur?”*, outlining twelve salient behaviors of intrapreneurs, Pinchot’s (1985, p. 31) sixth question reads: ”Are you able to keep your ideas under cover, suppressing your urge to tell everyone about them until you have tested them and developed a plan for implementation?” Keeping intrapreneuring *sub rosa* in part or entirely, to Pinchot, is more often than not a tactical necessity. Such practices could be recognized as evasive or deviant (and classified as shadow innovation), but more importantly here: if there is too much discrepancy between prognoses for and outcomes of intrapreneurial ventures, one can assume that trust depletes over false or erroneous imitation.

Literature on organizational transformation in general, and digital transformation in particular, can help understand the effects of intrapreneurship, and how ”digital intrapreneurs” (Pinchot & Soltanifar 2021) can be recognized as insider threats. Digital transformation is particularly relevant in contemporary research of intelligence services innovation as ”It is only a small exaggeration to say that software has eaten just about everything in the IC” (STAR 2020).

[10] Red links in Intellipedia (as on Wikipedia) links to pages that have yet to be published, essentially indicating that it would be nice for the subject to have a page of its own in the future.

6 Conclusion

To answer the research question *"How can intrapreneurs be recognized as insider threats?"*, this thesis has presented a number of perspectives drawn from literature
in the fields of economics, computer science, intelligence studies, law, and political science.

For illustrative purposes, these perspectives have been applied to a typical case of intrapreneurship in the intelligence services: Intellipedia. In proposing how different perspectives can assist understanding of how intrapreneurs are recognized as insider threats, their explanatory powers have been briefly explored rather than tested. Intellipedia is in this sense used to illustrate rather than to verify or falsify perspectives, as this thesis does not try to assess how or when recognizing intrapreneurs as threats might be justified or crucial.

6.1 Contribution to science

This thesis may serve as an orientation of unexplored or underutilised connections between scientific contributions to different fields, and of their relevance to the study of insider threats and intrapreneurship. Specifically, the connection between intrapreneurship, constructive and destructive employee deviance, and insider threats is a promising contribution. Also, in applying a Rogerian (rather than a Pavlovian) approach to the perspectives on intrapreneurs as insider threats, this thesis offers new insights to the field of intrapreneurship.

6.2 Managerial implications

This thesis also offers perspectives on intrapreneurship and more generally intra-organizational innovation for practitioners, applicable to risk assessments and innovation management.

6.3 Limitations

This thesis has not attempted to verify or falsify if all intrapreneuring pose insider-threats (or tend to do so), nor has it tested any theories on how or under which circumstances intrapreneurs could or should be regarded as insider threats.

To truly understand – *verstehen* (Weber 1904) – points of views where intrapreneurs are indeed recognized as insider threats, other methods than the literature review must be applied in research.

6.4 Suggestions for future research

This narrative literature review may serve many suggestions for future research. Apart from suggestions provided in the Findings chapter, Intellipedia deserves further research as a case of intrapreneurship and innovation in the USIC.

The similarities and differences between Lipsky (1980) and Pinchot (1985), their work and their reception by scholars and practitioners then and now also deserve further attention. Their descriptions of autonomous, almost defiant, professionals are interesting to compare and connect to their authors and time of publishing, as both street-level bureaucracy and intrapreneurship are quantitatively more recognized than ever in literature[11].

[11] See Google N-Gram viewer for comparison.

7 References

Allison, G. T. (1971) *Essence of decision: explaining the Cuban missile crisis*. Glenview, URL

Andrus, D. Calvin (2005), ”The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community”, Studies in Intelligence, Vol 49, No 3, September 2005, URL

Antoncic, B. (2003), ”Risk taking in intrapreneurship: translating the individual level risk aversion into the organizational risk taking”, *Journal of Enterprising Culture*, 11:1, March 2003, DOI

Antoncic, B. & Hisrich, R. D. (2003) ”Clarifying the intrapreneurship concept”, Journal of Small Business and Enterprise Development, 10:1, 2003, pp. 7-24, DOI

AR2 (1982) [as quoted by Ingesson, 2016] Arméreglemente del 2: Taktik, M7741-100611, *Chefen för armén och Försvarets läromedelscentral*.

Arnold, E. & Magia, S. (2013) ”Intrapreneurship in government - Making it work”, *Deloitte University Press*, URL

Augusto Felício, J., Rodrigues, R. & Caldeirinha, V.R. (2012), "The effect of intrapreneurship on corporate performance", Management Decision, 50:10, p. 1717-1738, DOI

Barney J. (1991) ”Firm Resources and Sustained Competitive Advantage”, *Journal of Management*, 17:1, p. 99-120, DOI

Bator, P. (1992) ”A Comment on ‘Young, Becker and Pike's 'Rogerian' Rhetoric: A Twenty-Year Reassessment’”, *College English,* 54:1, p. 85-87, DOI

Baumlin, J. S. (1987) ”Persuasion, Rogerian Rhetoric, and Imaginative Play”, *Rhetoric Society Quarterly*, 17:1, p. 33–43, DOI

Baumol, W. J. (1990) ”Entrepreneurship: Productive, unproductive, and destructive”, *Journal of Political Economy*, 98(5), p. 893–921, DOI

Bell, A. J.C., Rogers, B. M. & Pearce, J. M., (2019), “The insider threat: Behavioral indicators and factors influencing likelihood of intervention” International Journal of Critical Infrastructure Protection, vol. 24, March 2019, Pages 166-176, DOI

Benitez‐Amado, J., Llorens‐Montes, F.J. and Nieves Perez‐Arostegui, M. (2010), “Information technology‐enabled intrapreneurship culture and firm performance”, *Industrial Management & Data Systems*, 110:4, p. 550-566, DOI

Birkinshaw, J. (2003). ”The paradox of corporate entrepreneurship: Post-Enron principles for encouraging creativity without crossing the line”, *Strategy and Business*, 30:1, p. 46–57, URL

Bishop, M. and Gates, C. (2008) “Defining the insider threat”, *Proceedings of the Cyber Security and Information Intelligence Research Workshop*, May 12–14, 2008, DOI

Bitektine, A. (2011), ”Toward a theory of social judgments of organizations: the case of legitimacy, reputation, and status”, *Academy of Management Review*, 36:1, p 151–179, DOI

Bryman, A. (2012) *Social Research Methods 4th ed.*, Oxford University Press,

Bulmash, B and Winokur, M. (2020) "Entrepreneurial passion and turnover intentions: The role of intrapreneurship opportunities and risk tolerance", *2020 IEEE International Conference on Industrial Technology (ICIT)*, pp. 1205-1209, DOI

Campbell, M. (2012), blog post: “Disruptive Thinkers: Intrapreneurship vice Entrepreneurship – Why this Distinction Matters”, Small Wars Journal, URL

Cappelli, D. M., Moore, A. P. & Trzeciak, R.F. (2012), “The CERT Guide to Insider Threats”, Pearson Education, Inc., URL

Chomik, A. (2011) ”Making Friends in Dark Shadows: An Examination of the Use of Social Computing Strategy Within the United States Intelligence Community Since 9/11”, *Global Media Journal - Canadian Edition*, 4:2, p. 95-113, URL

Chomik, A. (2012) ”Spies Wearing Purple Hats: The use of social computing to improve information sharing inside the Intelligence Community of the United States”, *University of Calgary* (Unpublished master's thesis), DOI

Christopher, P. (1994). *The ethics of war and peace: an introduction to legal and moral issues*, Englewood Cliffs/Prentice Hall, URL

CIA (2008), ”Intellipedia Marks Second Anniversary”, press release, *CIA News and Information*, March 20, 2008 (accessed November 17, 2020), URL [now accessible through archive.org]

CIA (2009) ”Intellipedia Gurus Win 2009 Homeland Security Medal”, promotional text, cia.gov, published October 08, 2009, accessed December 02, 2020, URL [now accessible through archive.org]

CIA (2020), ”CIA Unveils Its First Ever Federal Lab” (press release), CIA News and Information, September 21, 2020 (accessed November 16, 2020), URL [now accessible through archive.org]

Clausewitz, C. (1832) [1997] *On war*, Wordsworth (p. 66–67), URL

Cordella, A. & Paletti, A. (2019) ”Government as a platform, orchestration, and public value creation: The Italian case”, *Government Information Quarterly*, 36:4, DOI

Creech, G. E. (2020) “‘Real’ Insider Threat: Toxic Workplace Behavior in the Intelligence Community”, *International Journal of Intelligence and CounterIntelligence*, DOI

Daft, R. (1983) *Organization theory and design*, West URL

Davis, J. H., Schoorman, F. D., Mayer, R. C. and Tan, H. H. (2000) ”The Trusted General Manager and Business Unit Performance: Empirical Evidence of a Competitive Advantage”, *Strategic Management Journal*, 21:5, p. 563-576, DOI

Davis, M. S. (1971) ”That's Interesting: Towards a Phenomenology of Sociology and a Sociology of Phenomenology”, *Philosophy of the Social Sciences*, 1:4, p. 309-344, DOI

Deleuze, G. & Guattari, F. (1987) *A Thousand Plateaus - Capitalism and Schizophrenia*, University of Minnesota press, URL (Originally published as ”Mille Plateaux”, volume 2 of ”Capitalisme et Schizophrénie” 1980, Les Editions de Minuit, URL)

Dennehy, S. (2008) ”Keynote Address: Implementing Intellipedia Within a ‘Need to Know’ Culture” (audio recording), *USENIX Association*, 22nd Large Installation System Administration Conference (LISA '08), URL

Dennehy, S. (2017) ”Federal Government Wiki Introductions: Intellipedia”, *EMWCon Spring 2017, March 8* (url), (video recording) via Youtube, published March 23, 2017, accessed December 10, 2020, URL)

Dirks, K. T. & Ferrin, D. L. (2001) ”The Role of Trust in Organizational Settings”, *Organization Science*, 12:4, p 450-467, DOI

Dixon, N. M. & McNamara, L. A. (2008), ”Our Experience with Intellipedia: An Ethnographic Study at the Defense Intelligence Agency”, *DIA Knowledge Laboratory*, republished by Dixon on her blog, *conversation matters*, accessed December 02, 2020, URL

Edmondson, A., (1999), ”Psychological Safety and Learning Behavior in Work Teams”, *Administrative Science Quarterly*, 44:2, pp. 350-383, URL

Encyclopædia Britannica, (2018) ”Wiki", *Encyclopædia Britannica*, published August 1, 2018, accessed January 4, 2021, URL

Elert, N. & Henrekson, M. (2016) ”Evasive entrepreneurship”, *Small Business Economics*, 47:95, p. 95-113, DOI

Elert, N. & Stenkula, M. (2020) ”Intrapreneurship: Productive and Non-Productive”, *Entrepreneurship Theory and Practice*, October, DOI

Eli, A. B. & Hutchins, J. (2010) ”Intelligence after Intellipedia: Improving the Push Pull Balance with a Social Networking Utility”, *Defense Technical Information Center* (Winner of DTIC’s 2010 Student Paper Competition), URL

Eyal-Cohen, M. (2019): “Innovation Agents”, Washington & Lee Law Review, URL

Ferrari, R. (2015) ”Writing narrative style literature reviews”, *Medical Writing*, 24:4, p. 230-235, DOI

Fischhoff, B, Lichtenstein, S., Slovic, P., Derby, S. L., Keeney, R. (1981) *Acceptable Risk*, Cambridge University Press, URL

Foss, K., Foss, N. J., & Klein, P. G. (2007) ”Original and derived judgment: An entrepreneurial theory of economic organization”, *Organization Studies*, 28:12, p. 1893–1912, DOI

Freeman, C. (1982) *The Economics of Industrial Innovation*, 2nd edn, Frances Pinter, URL

Galperin, B. L. & Burke, R. J. (2006) ”Uncovering the relationship between workaholism and workplace destructive and constructive deviance: an exploratory study”, *International Journal of Human Resource Management*, 17:2, p. 331–347, DOI

Galperin, B. L. (2012) ”Exploring the Nomological Network of Workplace Deviance: Developing and Validating a Measure of Constructive Deviance”, *Journal of Applied Social Psychology*, 42:12, p. 2988–3025, DOI

Garud, R. & Van de Ven, A. H. (1992) ”An empirical evaluation of the internal corporate venturing process”, *Strategic Management Journal*, 13:S1, p. 93-109, DOI

Goodson, P. (2010) *Theory in health promotion research and practice: Thinking outside the box*, Jones & Bartlett Learning, URL

Green, D. (2014) ”Insider Threats and Employee Deviance: Developing an Updated Typology of Deviant Workplace Behaviors”, *Issues in Information Systems*, 15:2, p. 185–189, DOI

Greitzer, F.L., Strozer, J.R., Cohen, S., Moore, A.P., Mundie, D. & Cowley, J., 2014, “Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits”, *2014 IEEE Security & Privacy Workshops*, p. 236, DOI

Hamel, G. & Zanini, M. (2018) “The End of Bureaucracy”, *Harvard Business Review*, 96:6, p. 50-59, URL

Hart, C. (1998) *Doing a literature review : releasing the social science research imagination*, Sage, URL

Hashmi, K.A. & Siddiqui, D.A. (2020), ”Antecedents of Employees' Entrepreneurial Orientation: The role of Organizational Culture and the Enabling Environment”, *Business and Economic Research*, 10:3, DOI

Havenstein, H. (2008) ”CIA Explains Intellipedia”, *Computerworld*, published June 10, 2008, accessed December 10, 2020, URL

Healy, K. (2017) ”Fuck Nuance”, *Sociological Theory*, 35:2, p. 118-127, DOI

Helmond, A. (2015) ”The Platformization of the Web: Making Web Data Platform Ready”. *Social Media + Society*, DOI

Hinings, B., Gegenhuber, T. & Greenwood, R. (2018), ”Digital innovation and transformation: An institutional perspective”, *Information and Organization*, 28:1, p. 52-61, DOI

Howard, A (2010) ”Intellipedia: Moving from a culture of "need to know" to "need to share" using wikis” (video recording), *O'Reilly youtube channel*, published June 1, 2010, accessed December 10, 2020, URL

Höyssä, M. & Hyysalo, S. (2009) ”The fog of innovation: Innovativeness and deviance in developing new clinical testing equipment”, *Research Policy*, 38:6, p. 984-993, DOI

Ingesson, T. (2016) ”The politics of combat : the political and strategic impact of tactical-level subcultures, 1939-1995”, *Lund University Publications*, URL

Ingesson, T. (2017). ”Trigger-Happy, Autonomous, and Disobedient: Nordbat 2 and Mission Command in Bosnia”, *The Strategy Bridge*, September 20, 2020, accessed December 10, 2020, URL

INSA, Intelligence and National Security Alliance, (2017) ”Assessing the mind of the malicious insider: using a behavioral model and data analytics to improve continuous evaluation”, *Security Policy Reform Council (SPRC), Insider Threat Subcommittee*, URL

Javorsek, D. II, Rose, J., Marshall, C. & Leitner, P. (2015) ”A Formal Risk-Effectiveness Analysis Proposal for the Compartmentalized Intelligence Security Structure”, *International Journal of Intelligence and CounterIntelligence*, 28:4, 734-761, DOI

Kennedy, N. & David, O. (2018) ”Outsourcing Deviance: When 3rd Party Technology Innovativeness Becomes a Threat to Information Systems”, *Open Innovations Conference (OI)*, p. 140-147, DOI

Kitrosser, H. (2008) ”Congressional Oversight of National Security Activities: Improving Information Funnels”, *Cardozo Law Review*, 29:3, p. 1049-1090, URL

Lardinois, F. (2009) ”Intellipedia: Intelligence Agencies' Wiki Suffers Midlife Crisis”, *The New York Times* (syndicated from *ReadWriteWeb*), published February 19, 2009, accessed December 10, 2020, URL

Lassner, P. (1990) ”Feminist Responses to Rogerian Argument”, *Rhetoric Review*, 8:2, p. 220-232, URL

Lipsky, M. (1980) *Street-Level Bureaucracy: Dilemmas of the Individual in Public Services*, Russell Sage Foundation, URL

Lukes, M. & Stephan, U. (2017) ”Measuring employee innovation : A review of existing scales and the development of the innovative behavior and innovation support inventories across cultures” *International Journal of Entrepreneurial Behavior & Research*, 23:1, p. 136-158, DOI

Magnusson, J., Koutsikouria, D. & Päivärinta, T. (2020), ”Efficiency creep and shadow innovation: enacting ambidextrous IT Governance in the public sector”, *European Journal of Information Systems*, DOI

Manjikian, M. (2020) “‘Those Clowns Out at Langley’: A Theory of Trust between the Intelligence Community and the President”, *International Journal of Intelligence and CounterIntelligence*, 33:4, p. 709-730, DOI

March, J. G. (1991). ”Exploration and exploitation in organizational learning”, *Organization Science*, 2:1, p. 71-87 (Institute of Management Sciences), URL

Margolin, L. (2020) ”Rogerian Psychotherapy and the Problem of Power: A Foucauldian Interpretation”, *Journal of Humanistic Psychology*, 60:1, p. 130–143, DOI

McLaughlin, J. & Dorfman, Z. (2019) ”'Shattered': Inside the secret battle to save America's undercover spies in the digital age”, *Yahoo News*, December 30, 2019 (accessed November 16, 2020), URL

Merriam-Webster (2021) “Perspective”, (online dictionary) *Merriam-Webster.com*, Accessed 9 January 2021, URL

Movahedian, G., Shabani, A., Cheshmesohrabi, M., Asefe, A. (2020) ”Explanation of the Rhizomatic Approach in Knowledge and Information Organization Systems with Emphasis on Web Space”, *Iranian Journal of Information Processing & Management*, 35:3, p. 817–846, URL

Mundie, D. A. Perl, S. & Huth, C. L. (2013), "Toward an Ontology for Insider Threat Research: Varieties of Insider Threat Definitions", *Third Workshop on Socio-Technical Aspects in Security and Trust*, DOI

Nicander, L.D. (2011) “Understanding Intelligence Community Innovation in the Post-9/11 World”, *International Journal of Intelligence and CounterIntelligence*, 24:3, 534-568, DOI

Nurse, J. R. C., Buckley, O., Legg, P.A., Goldsmith, M., Creese, S., Wright, G. R. T, Whitty, M. (2014) "Understanding Insider Threat: A Framework for Characterising Attacks", *IEEE Security and Privacy Workshops*, San Jose, CA, 2014, p. 214-228, DOI

Oliver, C. (2012) ”Critical Realist Grounded Theory: A New Approach for Social Work Research”, *The British Journal of Social Work*, 42:2, p. 371–387, DOI

Pâquet L. (2019) ”The #Rhetoric of Waleed Aly’s ‘Send Forgiveness Viral’: Is Rogerian argumentation an appropriate response to racism?”, *Argumentation & Advocacy*, 55:2, p. 152-168, DOI

Pedersen, T. & Jansen, P. T. (2019) ”Seduced by secrecy – perplexed by complexity: effects of secret vs open-source on intelligence credibility and analytic confidence”, *Intelligence and National Security*, 34:6, p. 881-898, DOI

Peled, A. (2016) ”Coerce, Consent, and Coax: A Review of U.S. Congressional Efforts to Improve Federal Counterterrorism Information Sharing”, *Terrorism and Political Violence*, 28:4, p. 674-691, DOI

Pfaff, T. & Tiel, J. R. (2004) ”The Ethics of Espionage”, *Journal of Military Ethics*, 3:1, p. 1-15, DOI

Pfleeger, C. P., Lawrence Pfleeger, S., Margulies, J., 2015, *Security in Computing*, ed. 5, Pearson Education, Inc., URL

Pinchot, G. & Pinchot, E. S. (1978) ”Intra-Corporate Entrepreneurship”, Tarrytown School for Entrepreneurs, (whitepaper), URL

Pinchot, G. (1985) *Intrapreneuring: Why you don’t have to leave the corporation to become an entrepreneur*, Harper & Row, ISBN: 0060913355, URL

Pinchot, G. & Soltanifar, M. (2021) “Digital Intrapreneurship: The Corporate Solution to a Rapid Digitalisation”. In: Soltanifar M., Hughes M., Göcke L. (eds) *Digital Entrepreneurship. Future of Business and Finance*. Springer, DOI

Rapoport, A. (1960) *Fights, games and debates*, Ann Arbor, University of Michigan Press, URL

Rogers, C. (2017) [1952] "Communication: Its Blocking and Facilitation", *ETC: A Review of General Semantics*. 74:1/2, p. 129-135, URL

Ryan, G. W. & Bernard, H. R. (2003), ”Techniques to Identify Themes”, *Field Methods*, 15, p. 85–109, DOI

Sanghvi, N. (1984) “In-House Entrepreneurship”, *Economic and Political Weekly*, 19:39, p. 1697–1697, URL

Shulsky, A. N. & Schmitt, G. J. (2002) *Silent warfare - understanding the world of intelligence*, 3rd ed., Potomac Books, URL

Schumpeter, J. A. (1942) [2003]. *Capitalism, Socialism and Democracy*, Taylor & Francis, URL

Scott, L. & Jackson, P. (2004) ”The Study of Intelligence in Theory and Practice”, *Intelligence & National Security*, 19:2, p. 139-169, DOI

STAR, U.S. House Permanent Select Committee on Intelligence's Subcommittee on Strategic Technologies and Advanced Research (2020), *Rightly Scaled, Carefully Open, Infinitely Agile: Reconfiguring to Win the Innovation Race in the Intelligence Community*, accessed December 5, 2020, URL

Suchman, M. (1995), ”Managing legitimacy: Strategic and institutional approaches”, *Academy of Management Review*, 20:3, p. 571–610, DOI

Tomlin, S. (2005) ”The expanding electronic universe”, *Nature,* 438:547, DOI

Trott, P. (2017) “Innovation Management and New Product Development”, 6th edn, *Pearson Education Limited*, URL

USAJOBS (2013), ”Intellipedia”, promotional video for U.S. federal employment, *Youtube*, published November 3, 2013, accessed December 10, 2020, URL

Voon, N. L., Othman, M. H. & Leng, C. S. (2019) ”Constructive and destructive workplace deviance: an review”, *International conference on social sciences and humanities (ICOSSH)*, 8 – 9 October 2019, URL

Warren, D. E., (2003), ”Constructive and destructive deviance in organizations”, *Academy of Management Review*, 28:4, p. 622-632, DOI

Weber, M., (1904) [2012] “Samhällsvetenskapernas objektivitet”, översättning S. & A. Andersson, *Tre klassiska texter*, Korpen Koloni, URL (Originally published as: ”Die ‘Objektivität’ sozialwissenschaftlicher und sozialpolitischer Erkenntnis”, *Archiv für Sozialwissenschaft und Sozialpolitik*, 19, URL)

Willbrand, R.T. (2010) ”The evolution toward ‘bureaucracy 2.0’: A case study on Intellipedia, virtual collaboration, and the information sharing environment in the U.S. intelligence community”. *IMSCI 2010 - 4th International Multi-Conference on Society, Cybernetics and Informatics*. p. 149-155.

Young, R. E., Becker, A. L. & Pike, K. L. (1970) *Rhetoric : discovery and change*, Hartcourt, Brace & World, URL

Yun, J.J.; Zhao, X.; Jung, K.; Yigitcanlar, T. (2020) ”The Culture for Open Innovation Dynamics”, *Sustainability*, 12:12, DOI

Zahra, S. A. (1991) ”Predictors and financial outcomes of corporate entrepreneurship: An exploratory study”, *Journal of Business Venturing*, 6:4, p. 259-285, DOI

Zand D. E. (1997) *The Leadership Triad: Knowledge, Trust, and Power,* Oxford University Press, URL

Figure screenshot from Elert & Stenkula (2020) are included with kind permission from Niklas Elert.