



Lars Nicander

New Threats – Old Routines

Bureaucratic adaptability in the security policy environment



Lars Nicander

Born 1953, Tånnö, Sverige

BA, Stockholm University, 1983

Senior Total Defence Course,

National Defence College, 1990

Since 1993 associated with the Swedish Defence University, and from 1998
Director for its Center for Asymmetric Threat Studies (CATS).



New Threats – Old Routines

Bureaucratic adaptability in the security policy environment

Lars Nicander

Security Studies
Department of Political Science
Åbo Akademi University
Åbo, Finland, 2015

Förord

Denna avhandlingsresa startade i december 2005 då jag deltog vid en disputation vid Åbo Akademi i Vasa. Här återknöts den trevliga bekantskapen med docent Steve Lindberg som jag tidigare träffat 1986 i Åbo när han var redaktör för Finsk Tidskrift. Jag arbetade då med säkerhetspolitisk långsiktssplanering på det svenska försvarsdepartementet. Vår delegation ville på väg till Helsingfors passa på att ta del av den så kallade Åbo-skolans då något kontroversiella perspektiv på finsk och rysk säkerhetspolitik, vilket kanske inte helt uppskattades av mer offentliga finska företrädare. Detta blev början till ett nära samarbete mellan den svenska Försvarshögskolan (FHS) och Åbo Akademi med antal gemensamma seminarier och föreläsningar om rysk säkerhetspolitik, nya samhällsliga hotutmaningar m.m.

Jag fick här allt fler propåer från Steve om att med min breda praktiska erfarenhet i bagaget även rätta till mitt akademiska CV med en doktors-titel. Det forskningscentrum jag förestår – Centrum för Asymmetriska Hot- och TerrorismStudier (CATS) – är inriktat på policyrelevanta studier med flera disputerade medarbetare och det skulle ju se bättre ut om chefen också var det. Då det i Finland till skillnad från Sverige är vanligt med statsvetenskapliga sammanläggningsavhandlingar skulle jag också i stort kunna fortsätta med mitt heltidsarbete vid FHS. Det faktum att jag tidigare hade skrivit några kortare akademiska artiklar användes som argument om att jag redan hade kommit en bra bit på väg för en artikelavhandling – vilket dock självklart visade sig vara en sanning med mycket stor modifikation. Jag gav dock efter och blev våren 2008 antagen som doktorand.

Beträffande ämnet så har jag under drygt 20 år i arbetslivet har haft möjlighet att studera kopplingen mellan hot och planering inom det svenska säkerhetspolitiska systemet – särskilt de nya hoten mot informationssamhället. Insikten har blivit allt starkare om att även om nya hot visserligen kan uppmärksammas inom rimlig tid – inte alltid dock från de underrättelse- och säkerhetsorgan som har till uppgift att följa detta – så är det en än svårare och mer trögflytande process att få denna insikt planeringsgrundande för samhällsberedskapen. Devisen ”tvärsektoriella hot kräver tvärsektoriella lösningar!” är fortfarande tämligen utopisk i praktisk politik, varför jag önskade djupdyka i de bakomliggande processerna och fann att dessa aldrig syntes ha akademiskt tydligt beskrivits och än mindre granskats.

När jag nu efter många års hårt arbete ska sätta punkt för avhandlingssprocessen med en disputation så är det ett antal personer som särskilt bör framhållas och tackas för det stöd jag fått i denna arbetsprocess. Först och främst vill jag tacka min kloke och tålmodige handledare och vän docent Steve Lindberg, vilken som ovan nämnts är upphovet till denna avhandling. Många ”nötter” har knäckts vid sommarstället i Nagu där den vedeldade bastun frigjort tankeverksamheten. Stort och varmt tack Steve!

Likaså vill jag tacka professor Göran Djupsund som med sitt eminenta sinne för struktur alltid var snabb med att få ordning, pedagogik och logik i framställningen. Det har varit ett sant nöje och en förmån att få delta i de forskarskolor i Portugal och på Kreta som han lättsamt och med ständig intellektuell spänst drivit. Den trevliga stämning och ömsesidiga respekt som präglade såväl ledning som doktorandkollegor är här minnen för livet. Stort tack för detta Göran!

Då jag varit distansdoktorand har jag också behövt bollplank och stöd i Sverige. Jag vill här särskilt framhålla Dr. Greg Simons, Uppsala universitet, som varit ett omistligt stöd – inte minst vid den språkliga och formmässiga utformningen av de större artiklarna och enkäterna.

Likaså förtjänar forskningsassistent Linnéa Arnevall vid FHS/CATS ett varmt tack för de otaliga omformateringarna, referens- och bibliografi-uppställningarna m.m. där hennes kritiska nogksamhet är något varje forskare önskar som stöd. Medarbetaren och kollegan doktor Magnus Ranstorp har även bidragit med glada inspirerande tillrop under processen.

Ett särskilt omnämnande för stöd med viktiga kontakter i samband med min enkätundersökning rörande think tanks i USA går också till Dr. Greg Treverton, US National Intelligence Council – tidigare verksam vid RAND Corporation och tillika gästprofessor vid FHS/CATS.

Jag vill även särskilt tacka fakultetens förhandsgranskare av mitt manuskript – docent Tomas Ries vid Åbo Akademi och docent Mark Rhinard vid Stockholms universitet – som under maj-juni i år tog sig tid att läsa och granska mitt manuskript och i augusti leverera var sitt utlåtande. Det var både med glädje och ödmjukhet jag tog del av era insiktsfulla och sakliga yttranden.

Jag måste här också tacka Försvarshögskolan där mina institutionschefer – tidigare professor Bengt Sundelius och nuvarande chefen överste Jan Mörtberg – varit starkt uppmuntrande och bägge bidragit till att jag kunnat få tid och resurser för mitt avhandlingsarbete. En viktig extern finansieringskälla har också varit Myndigheten för samhällsskydd och beredskap (MSB) som med sitt miljöstöd till det forskningscentrum jag ansvarar för vill öka det akademiska intresset för dessa näraliggande frågor.

Slutligen vill jag också rikta ett tack till min hustru som burit en stor börda då helger och semestrar inte kunnat ägnas åt familj och barn när mina tankar varit fokuserade på helt andra områden.

Stockholm den 7 oktober 2015

Författaren

Table of contents

A. Introduction	9
1. Changes in the International Security Environment	9
2. Dissertation template.....	12
2.1. Research question.....	16
2.2. Definitions.....	17
2.2.1. Intelligence	17
2.2.2. Knowledge Monopoly	18
2.3. The security policy arena	19
2.4. The Process.....	20
2.5. Delimitations.....	22
2.6. Research and literature review.....	23
2.6.1. Threat/detection (Intelligence)	24
2.6.2. The policy process (“the Missing Link”)	25
2.6.3. Implementation/bureaucracy	28
2.6.4. Summary research design	30
3. Policy adaption within the national security environment.....	31
3.1. The model of analysis for security policy (“the decision chain”).....	31
3.2. Challenges for the security policy process concerning new threats	34
4. What processes are studied and how?	36
B. The articles	43
1. Shielding the net – understanding the issue of vulnerability and threat to the information society	43
2. Understanding Intelligence Community Innovation in the Post-9/11 World.....	64
3. Information Terrorism – When and by Whom?.....	98
4. The Trojan Horse in the Information Age.....	111
5. Think Tanks:	123
5.1. The role of Think-Tanks in the US Security Policy Environment – A Forgotten Actor?.....	123

5.2. The Recipe for Think Tank Success: From the Insiders Perspective	145
C. Summary & Conclusions.....	183
1. Findings	183
1.1. Article 1	183
1.2. Article 2	184
1.3. Article 3	184
1.4. Article 4.....	185
1.5. Article 5.1 and 5.2	185
1.6. Conclusions of article findings	186
2. Differences depending on policy impact – an alternative case?	188
3. The role of Think Tanks.....	190
4. Afterword.....	192
D. Sammanfattning.....	195

List of Figures (parts A & C)

Figure 1: Contrasting Intelligence and Policy Cultures ..	27
Figure 2: Analysis model Intelligence-Policy- Implementation.....	32
Figure 3: Relations Intelligence-Policy.....	36
Figure 4: Relations Policy-Bureaucracy	37
Figure 5: The impact of think tanks in the policy process.....	37
Figure 6: Ideal Case.....	183
Figure 7: Tainted case	188

Abstract

Within the framework of state security policy, the focus of this dissertation are the relations between how new security threats are perceived and the policy planning and bureaucratic implementation that are designed to address them. In addition, this thesis explores and studies some of the inertias that might exist in the core of the state apparatus as it addresses new threats and how these could be better managed.

The dissertation is built on five thematic and interrelated articles highlighting different aspects of when new significant national security threats are detected by different governments until the threats on the policy planning side translate into protective measures within the society. The timeline differs widely between different countries and some key aspects of this process are also studied. One focus concerns mechanisms for adaptability within the Intelligence Community, another on the policy planning process within the Cabinet Offices/National Security Councils and the third focus is on the planning process and how policy is implemented within the bureaucracy. The issue of policy transfer is also analysed, revealing that there is some imitation of innovation within governmental structures and policies, for example within the field of cyber defence.

The main findings of the dissertation are that this context has built-in inertias and bureaucratic seams found in most government bureaucratic machineries. As much of the information and planning measures imply security classification of the transparency and internal debate on these issues, alternative assessments become limited. To remedy this situation, the thesis recommends ways to improve the decision-making system in order to streamline the processes involved in making these decisions.

Another special focus of the thesis concerns the role of the public policy think tanks in the United States as an instrument of change in the country's national security decision-making environment, which is viewed from the perspective as being a possible source of new ideas and innovation. The findings in this part are based on unique interviews data on how think tanks become successful and influence the policy debate in a country such as the United States. It appears clearly that in countries such as the United States think tanks smooth the decision making processes, and that this model with some adaptations also might be transferrable to other democratic countries.

Keywords: Threat, Security Policy, Policy Transfer Analysis, Intelligence, Bureaucracy, Think Tanks.

Acronyms (part A & C)

CFR	Council on Foreign Relations
CIA	Central Intelligence Agency
CIIP	Critical Information Infrastructure Protection
CRS	Congressional Research Service
DCI	Director of Central Intelligence
DHS	Department of Homeland Security
DNI	Director of National Intelligence
ETA	Euskadi ta Askatasuna
FBI	Federal Bureau of Investigation
GWOT	Global War on Terrorism
IC	Intelligence Community
IPCC	International Panel on Climate Change
NGO	Non-Governmental Organisations
NPM	New Public Management
PDB	President's Daily Brief
PDD	President's Decision Directive
PIRA	Provisional Irish Republican Army
RIA	Revolution in Intelligence Affairs
RMA	Revolution in Military Affairs
SIS	Secret Intelligence Service
UK	United Kingdom
US	United States

A. Introduction

Globalization, and not least the development of a modern information society, has resulted in a general prosperity and economic and political development for many societies, but it has also resulted in new types of vulnerabilities and societal cross-border threats by those opposed to them. This development has given rise to new types of threats and challenges for national security policy considerations, which in turn requires new types of adaptability by policy and planning departments. Do governmental bureaucracies currently anticipate and plan relevant protective measures against the spectrum of such threats in a timely manner?

Within the framework of state security policy, the focus of this dissertation is on the relations between how new threats are perceived and the policy planning that is designed to meet them. The purpose is to study the inertias that might exist in the core of the state apparatus and how these could be better managed. In short, the added value of this approach is that it provides the combination of a cross-sectorial approach and up-to-date unique research data, all within a theoretical-empirical nexus to operationalize them. The intended result is to establish new knowledge and understanding and thus hopefully better support national security planning processes within governments.

1. Changes in the International Security Environment

The main focus of this dissertation is bureaucratic adaptability within the sphere of security policy in relation to developments in the international environment. In the shadow of the balance of threat from 1945-1991, the security policy environment created, perhaps paradoxically, the feeling of stability and safety, as well as predictability between East and West. The fall of the Berlin Wall, the break-up of the Soviet Union, the liberation of the former members of the Warsaw Pact in Eastern Europe, and Germany's unification brought security political détente, as well as economic development in Europe and globally. In his article, *The End of History*, Francis Fukuyama (1989) wrote about the end of ideologies in a multipolar world resulting from the end of the Cold War, and thereby the end of war between countries.

However, simultaneously, other types of religious, ethnic and territorial conflict issues, previously contained by the larger bipolar balance of power, were set loose. The United States sensed this development when it was discovered that they in fact had more enemies than before, as expressed by then-CIA director R. James Woolsey in 1993: "We have slain a large dragon. But we live now in a jungle filled with a bewildering variety of poisonous snakes. And in many ways, the dragon was easier to keep track of."¹ (Garthoff, 2007:221).

1 In testimony before the SSCI, 2 February 1993, just before his installation as DCI. The colorful metaphor provided a "sound-bite" justification for his view that substantial intelligence resources were still needed in the post-Cold War era" (Garthoff 2007:221).

Over the period from 1991 until early 2015, one of the most important changes in the international environment has been the change in security and defence policy, as well as the need for incorporating a more extensive threat picture when defining the components of societal security. This change has led to a more extensive concept of security with the addition of emerging threats such as increases in economic competition, climate change, migration flows, energy and oil dependency, terrorism, IT/cyber threats etc.

We now live in a new world order with the United States as the only super power, though maybe in the future challenged by an emerging China. The development has also dismantled borders, increased trade and has led to more integration between economies as well as individuals. Economic, as well as trade, developments have led to new equilibriums, and nowadays, previously poor and underdeveloped countries such as China, South Korea, Brazil, and India etc. are economic powers with an emphasis on high-tech development and growth. Today, it is primarily Africa that lacks its own infrastructure, and currently there is a race between companies, mainly from China and France/United States, over economic influence in regions such as Africa and elsewhere – hence, increasing competition over security policy (Brookes & Shin, 2006).

The flipside of largely positive technical and industrial development are the problems they contribute to an increasingly complex set of security policy options to address them. Increasing industrialization without balanced frameworks cause carbon emissions, increasing temperature levels, contaminates land, environmental degradation and climate change. Problems that in substance are uncontested (except among some fundamentalist circles in the United States over climate change), however, are not always well understood by policy makers in terms of their scope and their size (Gromet, Kunreuther, & Larrick, 2013; Hmielowski et al., 2013).

The UN's climate panel (IPCC, 2014) has pointed to the trend of extreme weather including storms, droughts in Africa that ruins harvests which in turn causes displacement of people, as well as melting glaciers and the reduction in sources of drinkable water etc. Against this background, the phenomenon of widespread economic refugees fleeing Africa, in search for a better life in the EU, has become increasingly evident over the past five years. Furthermore, these trends can also be translated into changes in security policy power relations – especially, at the regional level, as governments attempt to cope with such an upsurge in refugees.

In addition to the impact of climate change on regional security policy relationships, the supply of energy also has a clear security policy dimension. In Europe, the so-called energy weapon – primarily threats of reduction in or loss of gas supplies from Gazprom – has been used by Russia to not only affect countries in its immediate neighbourhood, but also other European countries such as Germany, France etc. that now are linked to the extensive system of gas pipelines from Russia (Paillard, 2010; Grigas, 2013; Daily Mail, 2009).

Another issue is the oil resources of the Middle East with its links to the conflicts between Iran and other Arab countries, as well as the conflict between Israel and Palestine, to mention two examples. Western economic dependence on oil from the Arab countries has also been one of the foundations for the rise of the Islamist movements that protested against their totalitarian regimes, as well as the perception of an unhealthy influence of Western values over their societies. Earlier, paradoxically, the United States opposition to the Soviet occupation in Afghanistan led to a collision course after the first Gulf War in 1991 when American bases were located in Saudi Arabia, thereby helping to mobilize al Qaeda against the U.S.

In turn, this led to an upsurge in fundamentalist and religious revival in which several Muslim countries imposed political Islam and an extreme interpretation of Sharia law. The concrete threat consisted of the growth in extreme Islamic terrorism with Al-Qaida and 9/11 as main features, but also resulted in a comprehensive multi-pronged threat of terrorism. The militant Sunni movements also pose a serious threat to the states in the Middle East and Africa in which they operate, e.g. Iraq/Syria, Nigeria, Mali and Somalia/Kenya (Pham, 2012; Burke, 2004; Sergie & Johnson, 2014; CNN, 2014).

Countermeasures against international terrorism, with the perceived stigmatization of Muslims (see for example Simons, 2010, for example) as well as second and third generation of immigrant youths in Britain, France and other Western countries being attracted by the new Islamic identity, has also evolved into a myriad of societal problems. It is worth noting that youths from excluded and segregated areas in Western European cities tend not to be the typical Islamist terrorists, as these have generally been well-educated from middle-class backgrounds as in the case of the two multi-pronged attacks in London in July 2005 (Brighton, 2007), which were carried out by operatives previously considered to have been well integrated. As for causes of violent radicalization there are varied socio-economic backgrounds behind them.

In addition to previously mentioned changes, globalization has also resulted in the development of the information society and our IT dependence, which in turn has led to economic growth as well as opening up for democratic movements in previously politically closed countries. On the flipside however, is the increase in possibilities for digital espionage and surveillance by governments, as well as direct threats by adversaries against a society's critical information infrastructure. Technological and economic development comes before safety, and it is both difficult and expensive to patch up existing systems. The integration and interdependence that has evolved in-between, for example electricity and telecommunications infrastructure built upon IP protocols, has created windows of vulnerabilities not anticipated (PCCIP, 1997). An example of this is the trend towards "Internet of Things" and "Smart Grid" in which refrigerators and electricity consumption at home and in larger substations is controlled via the Internet.

The information society has also created opportunities to upgrade the capability of counter terrorism to monitor suspicious individuals' movements and communication patterns with so-called "big data" analytics.² Additionally, threats of economic espionage and sabotage from state actors can also be added to this list of new vulnerabilities in modern society.

The countries in Europe – particularly the Nordic countries – that during the Cold War considered themselves to be at risk of armed aggression from the Soviet Union have to a large degree kept their heritage with a total defence concept where their civil infrastructures had a large degree a built-in redundancy. These countries are therefore relatively less vulnerable to accidental or deliberate large-scale IT failures than other countries (Rantapelkonen & Salminen, 2013).

Yet another change in the international environment is global cooperation due to endogenous incentives such as international crisis management via the EU, G8 and others (Boin, Ekengren & Rhinard, 2013). The UN has also become more active in granting mandates for armed interventions in Afghanistan as well as in Africa, in order to help resolve those conflicts. Increased European integration through common foreign and security policies in the EU via the Maastricht and Lisbon treaties have changed the conditions of reacting during a crisis radically as well as with other problems outside national borders.

Geopolitically, Russia has after its relative democratization and economic decline in the 1990s, begun to recover. Events in Ukraine during the spring of 2014 indicated that President Vladimir Putin seeks to recapture the superpower role of the former Soviet Union in the international arena based on its possession of nuclear weapons and an invigorated totalitarian society (Speck, 2014).

2. Dissertation template

In this dissertation the entire process within security policy is covered with a certain emphasis on the role of think tanks as elements within an innovative model to compare and draw lessons from on how such private sector think tanks can contribute to improving policy making in their societies. The US was chosen as a role model because of the constructive role that such think tanks play in its society, hence it is the focus on the thesis, also owing to its dominant role in international politics and innovative ways of generating ideas, practices and policies (McGann, 2007). This is posited to provide a template for other countries to follow. This is the first step, to identify those aspects that facilitates or hinder the policy process, the rest is for future research.

Conceptually, the policy process can be divided in three sub-areas. The first one is the "policy making environment" (e.g. Cabinet offices, National Security Council structures etc.) within the political and administrative centre in the state apparatus (**B**). The second one (**A**) is the "input" environment (e.g. intelli-

2 The collection of large amounts of data to be able to find new information and correlations would otherwise be hard to access.

gence services). The third sub-area (C) is the “output” environment (executive agencies and authorities).

Consequently, the “policy making environment” indicates those decision-making and administrative settings within the state apparatus in which threat assessments are linked to counteractions and protection, as well as the formulation of relevant policies. The policy making environment can also in its turn be divided into three subparts – the first constituting the customer/client function to the intelligence community (B1), the second part dealing with the decision-making weighed upon political preferences and economic/budgetary consequences (B2), and the third is the planning part that sends sharp and clear signals to the administration/bureaucracy so that decisions are adopted and implemented as intended (B3).

The purpose of focusing on the policy environment is to study the interaction and linkages between, on the one hand, state institutions which have to be on the alert and warn of various forms of antagonistic threats, and on the other hand, the structures planning for community preparedness whose function is to quickly and seamlessly convert these signals into steering directives along with corresponding resource allocations to vulnerable sectors. The requirement for greater speed in this process has increased dramatically in the information society in which yesterday’s routines are not suited for today’s new threats and vulnerabilities. Therefore, studies of mechanisms that can affect the speed of the process are highly policy relevant.

Evans and Davies (1999:361), in an attempt to understand policy transfer remark on the diffuse nature of the field. They note that a variety of disciplines are used, and researching policy transfer has a multi-disciplinary character. There are similar research agenda across different disciplines, however, the findings often do not connect and can talk past each other (Evans & Davies, 1999:361). It is noted that “a sound model is not necessarily one that purely explains or predicts with precision. It is one rich with implications. [...] But in order to make stronger knowledge claims it must engage in theoretical and methodological pluralism and integration” (Evans and Davies, 1999:364). In a similar vein, this thesis has chosen to take a multi-disciplinary approach over any single discipline. It is hoped to gain a greater level of explanatory value by avoiding the pitfall of an individual and unitary theory approach that could result in missing the bigger picture through talking past each other. Ultimately, the thesis seeks to enrich the implications of research in this field of study.

Since there are currently no identified theories that describe incentives for change within closed monopolies of the state apparatus’s innermost core, the dissertation proposes a new conceptual framework. Hence this dissertation attempts to fill this void in which decisions-making processes and its bottlenecks³ are studied from the very beginning to the very end of the process.

3 Bottlenecks refers here to knowledge monopolies, change aversion, insufficient administrative priorities etc. The chain of decision can partly be due to actual exogenous differences

Besides this, existing theories are evaluated through the empirical application of interviews with experienced practitioners in the field of security policy. Consequently, the dissertation does not only summarize the state of the research today, but also challenges the research aspects of the current state of the art on the security policy decision-making process.

An important supposition in the dissertation is that greater pluralism – on both understanding the threat and the planning side in addressing it – contributes to an increased willingness to change regarding the implementation of prompted measures as well as change in the administrative/bureaucratic structures. This is partly based on the comprehensive discussion that, among others, Max Weber (1922) presented about the value of a certain overlap between sectors even in a very limited state apparatus, as well as based in the contemporary debate between monists and pluralists. Therefore, the balance between thinking correctly in relation to thinking freely is discussed frequently in an American administrative/bureaucratic context with a politicized administration.⁴ The most basic rationalist argument for systematic pluralism appears frequently in the economic context, enabling additional insights and thereby reduces the risk that any aspect is not sufficiently illuminated (Stiglitz, 1999).

Thus, a lack of pluralism in the policy planning process could lead to an inadequate and suboptimal utilization of resources to the detriment of taxpayers and the state interest. The balance between government offices (the customer/client) and government agencies (the producers) can also be skewed in systems with small cabinet departments and strong autonomous agencies.

In this dissertation the question of policy making pluralism is tied to studies and strategies for protection of various military defence systems and civilian critical information infrastructures that are connected to the electrical and telecommunication systems. A special relation here is that these processes predominantly take place in a closed system with a knowledge monopoly in which external influence (“peer review”, market mechanisms etc.) is almost non-existent.

The structure of the dissertation consists of a general introduction, as well as five articles that in different ways illustrate some problems and core issues concerning the link between “threat” and “planning” at the national level - two of which are shorter and more indicative whilst three are more profound. The conclusions from the three more profound main articles then become pieces of the puzzle in the concluding part. In turn, the fifth and last long article is divided into two parts, one is more theoretical and one is more empirically

in various countries’ legal and constitutional systems, but the interesting thing is if there also are endogenous general phenomena that contributes to reducing or delaying the type of specific decision-making processes that are studied.

4 A more theoretical discussion on the value of monism vs. pluralism within state bureaucracy/administration can be found in both Weber (1922) and in Michael W. Spicer’s article Value pluralism and its implications for American public administration (2001).

oriented. Finally, a concluding chapter attempts to identify the bottlenecks that may exist in this type of planning.

Although the reasoning is primarily intended to be applied in a smaller market economy and countries with developed information technology, such as Sweden, several illustrations are gleaned from the United States due to the relative transparency in handling these issues there (Hastedt, 1991).

The research field on this approach is generally understudied – possibly because the research question cuts across several academic disciplines (international relations, public policy/public administration, economics, law etc.). One relatively new academic school of thought of use here is “Policy Transfer Analysis” (Evans & Davies, 1999:361) that has a cross-sector approach, though no corresponding cross-sector theories adapted to the scope of this dissertation yet have been identified.

Hence, hopefully, this dissertation’s conceptual framework will result in new inter-disciplinary knowledge, and also might be considered as a “critical ontological turn” as these relationships and activities within the core of government apparently seems to have received little if any systematic scholarly attention.

In 1929, Martin Heidegger discussed the issue of the critical ontological turn, which necessitated an investigation of the nothing:

Man’s existence as Dasein inherently elevates the legitimacy of the nothing to unseen standards in western “logic.” Questioning the nothing recognizes the nothing as a practice of philosophy and alludes to the main criterion of Heidegger’s existentialism: the Dasein of existence. Any choice immediately throws the subject into responsibility, but affirmation lies at how one orients himself to the human nature of Dasein – and tangentially, to the nothing [...] Affirmation, then, lies at the ability of the free subject to hold themselves to the nothingness – or, the search of an authentic subjectivity that is revealed through this practice (Zausen, 2014).

Therefore, affirmation is about the ability to find the authentic in face of the obstacle of nothingness.

A quest for knowledge begins when the existing knowledge in the social and political environment loses its legitimacy or usefulness (Beal, 2011:56-57). “Affirmation is a sought existence, a reaction to the infinite antagonisms to which the free subject necessarily must interact. Subjectivity invokes a search for overcoming the unauthentic in search for the authentic, in the face of the nothing” (Zausen, 2014).

The political underpinnings of our ontological model need to be thoroughly scrutinised as failing to do so may result in alternative possibilities being missed or excluded, which necessitates a critical approach being undertaken (Beal, 2011:57). It is a matter of projecting experience of the nothing towards the subject in order to locate the nothing through experiencing it. “Ontology is always in motion and never static; it is a relation of subjects with objects, and the outcome of this interaction” (Zausen, 2014). The political and theoretical potential of ontology is found not only in the present, but also the influence

of the past, which is particularly relevant in the sphere of social (and political) transformation (Beal, 2011:62).

Within the context of this thesis, this is a question and a matter of an individual or organisation and their ability to make sense and create an understanding of an unknown environment, and therefore, to shape and influence a competitive edge in a highly contested political environment.

2.1. Research question

As mentioned earlier the purpose is to study the inertia (“bottlenecks”) that exists in the core of the state policy making apparatus and how it could be better managed. Thus the main research question at heart is to be formulated as: ***From the discovery of a new threat until the implementation of policy to address the problem, what variables affect the policy planning process and how?***

Related to the main research question three sub-questions are developed:

- How are security policy threats evolving and perceived in the post-Cold War era?
- Do these threats stimulate innovation and change in government bureaucracies as well as policy formulation and implementation?
- What are the main obstacles/problems in addressing the new threats?

The first sub-question relates to the security policy arena where as the two other sub-questions deal with the policy process and the responsible state machinery. These three sub-questions connect to the research focus and questions in the articles that form the part B of this thesis.

The first article (*Shielding the Net – understanding the issue of vulnerability and threat to the information society*) focuses on the timelines from detection of a threat to implementing necessary safeguards, and thus are related to the sub-questions 1 and 3.

The underlying research question in the second article (*Understanding Intelligence Community Innovation in the Post 9/11 World*) is about innovation in closed government policy making environments, and thus relates to sub-question 2 above.

The third article (*Information Terrorism – When and by Whom?*) elaborates on possible venues of innovative terrorist modus – i.e. when will terrorists attack the vulnerabilities within the information societies – and here relates to sub-question 1.

The fourth article (*The Trojan Horse in the Information Age*) focuses on the new threat environment and the need for changed approaches compared to the Cold War-era.

Finally, the two last articles (*The role of Think Tanks in the US Security Policy – A Forgotten Actor?* and *The recipe for think Tank Success: From the Insiders Perspective*) poses the research questions “Do Think Tank influence Security

Policy?” and “How do they do it and become successful?”, which relates to all three sub-questions.

2.2. Definitions

In order to understand the subject there are two processes that need explanation, firstly, “Intelligence”, and secondly, “Knowledge Monopoly”.

2.2.1. Intelligence

There are several categories of definitions of intelligence where the two most important take their stance in *what is done* and others in *what type of activities* that are included. The focus for this dissertation is in intelligence that is used in support of foreign and security policy. The intelligence methodology itself can of course also be applied to security intelligence, criminal intelligence and business intelligence. As a business concept, there should always be a demand/customer – most often the highest levels of decision-making (Armed Forces Head Quarters, Cabinet Offices) that handles military or foreign issues. Nowadays, finance and trade departments are often considered a customer as information in these areas affects a country’s “economic well-being” as the British SIS describes their task (SIS, 2015).

One example of the first category mentioned above, intelligence as a method and what is being done, is to systematically process, analyse and disseminate information (data) to make sense and create knowledge. “The function of institutionalized intelligence is to centralize, process, and disseminate information useful to the formation and implementation of a foreign policy.” (Marrin, 2002:1).

Michael Warner (2007) provides an even more distinct version: “Intelligence is secret, state activity to understand or influence foreign entities.”

A more interpretive definition in the same category is “...the umbrella term referring to the range of activities – from targeting through information gathering to analysis and dissemination – that are conducted in secret and aimed at maintaining or enhancing security by providing forewarning of threats or potential threats in a manner that allows for the timely implementation of a preventive policy or strategy.” (Gill & Phytian, 2004:1).

An example of the second category definitions mentioned above, about activities included, in an American context is provided by Shulsky and Schmitt (2001) in *Silent Warfare* when they divide intelligence into four parts – collection, processing/analysis, security intelligence and “covert action” (e.g. paramilitary activities).

A more official US definition can be found in the CIA’s *A consumer’s guide to intelligence* (1995:vii):

Reduced to its simplest terms, intelligence is knowledge and foreknowledge of the world around us - the prelude to decision and action by US policymakers. Intelligence organizations provide this information in a fashion that allows consumers, either civilian leaders or military commanders, to consider

alternative options and outcomes. Above all, the analytical process must be rigorous, timely, and relevant to policy needs and concerns.

In a traditional European context “covert action” is not included as this is considered part of the executive policy implementation. Likewise, specifically in-between American and British intelligence, there is a difference in emphasis in regards to “raw intelligence” being delivered straight up to the highest political level in the UK. This rarely occurs in the United States where the intelligence is processed and contextualized into the information that thereafter for example is presented in the President’s Daily Brief (PDB). A further distinction is that the main activities are collection and analysis – not “counter intelligence” – as the security intelligence service rather is a related sub-discipline for foreign intelligence service.

Thus, the intelligence community is a producer of fact-finding and assessment reports and according to all available theory separated from the policy environment and the decision-making process, or to use a British expression “on the tap but not on the top”.

2.2.2. Knowledge Monopoly

The term knowledge monopoly has primarily been described in the literature on “Knowledge Management”, and has sometimes been linked to public administration. Knowledge Management describes information in three layers of an increasingly higher degree of processing – data, information and knowledge (Easterby-Smith & Lyles, 2003b:1-15).

Within crisis management literature the focus is on the sub-division “organizational learning” which attempts to identify what knowledge is available, and especially where about in the system in the context of time-critical externally generated events. However, this area is also useful here. Knowledge here is twofold – first, the formal knowledge (“explicit knowledge”) possessed by an individual obtained through for example training and/or holding a specific position, and secondly, the informal “silent” knowledge (“tacit”) is also central. It is not always enough to have the recipe for a cake; it is a completely different thing to be able to bake it (Koraeus, 2008).

Thus, an ideal organization learns to pass on even “silent” knowledge – tacit, which likewise can be applied in a closed national security system as outlined in the so-called SECI-model “socialization, externalization, combination, internalization” (Nonaka & Toyama, 2003).

A potential problem may be that the bureaucrats in the administration get the upper hand as Max Weber (1922) described, and as subsequently developed by William Niskanen Jr. (1994). Niskanen was one of the leading representatives who supported the Reagan administration when contextualizing the concept “New Public Management”, which sought to have a minimal state apparatus and outsourced public services. However, Niskanen pursued specialization between the government agencies that would remain at the state’s core, as this

would more clearly demonstrate where tax money provided the best results in relation to agencies undertaking servicing tasks that overlap.

In this context, Niskanen described the concept of “knowledge monopoly” as a “bilateral monopoly” where the administrator within the bureaucracy/agency always had the upper hand against the more budgetary focused sponsor organization (“policy environment”/Cabinet Offices). “All or nothing”-proposals were often proposed, in which the agencies often got their requests approved, as the representatives from the sponsor organization seldom could call the cards (Lindroos, 2013). It should be added that this was before the big public budget cuts in the United States undertaken in more recent years.

2.3. The security policy arena⁵

The main institutional actors in the state apparatus that traditionally are involved in the design and implementation of security policy are the foreign and defence ministries, while the armed forces and other foreign service agencies as well as the strategic intelligence services – if not included in any of the sectors above – are implementing. The Prime Minister and the President’s offices respectively has always by definition a role in this – not least for the EU Member States where much of the coordination takes place at this level.

At the margin, other parts of the state apparatus can be included in the implementation, such as the judicial sphere with the Department of Justice, police and security services, as well as trade policy functions with export control agencies and the Department of Finance concerning economic aid and sanctions. Generally, parliaments are quite marginal in these contexts; however, the Congress in the United States, as a non-parliamentary legislature, is a case of exception.

Security policy decision-making can roughly be divided into three levels – territorial defence, diplomacy and trade, and international security cooperation including transnational threats. The first – often seen as the hard core – is about different types of threats to the nation’s survival in the context of war, which concerns the design of the nation’s military power resources as well as any agreements with other countries on defence and security assistance. The main participants are the Department of Defence and Armed Forces as they are responsible for concrete aspects of defence planning. As terrorism and cyber threats now are for real the department/agencies concerned with Justice and Homeland Security must also be included (Clapper, 2015).

The second level involves, on the one hand, actions vis-à-vis other countries in the peacetime international environment – especially actions linked to the country’s geographical neighbourhood – as well as diplomatically and economically coordinated responses to potential threats from other countries. It can comprise military exercises in disputed maritime areas to mark attendance at

⁵ For more information on Swedish government administration please see Bäck et al. (2011:170-217) and Petersson (2006).

an economic zone or stabilizing possible impeding developments that may prevent freedom of navigation and transport.

On the other hand, on the second level there are also jointly coordinated sanctions against a state that behaves in an unacceptable and destabilizing manner in the neighbourhood. One example of a relatively harsh economic marker is the economic sanctions imposed by the EU and others against Russia due to the developments in Ukraine in the spring of 2014. The events in Ukraine clearly demonstrate that dimensions of economic and trade policy nowadays are used as tools in security policy to pressure nations, in which arms export (France), gas (Germany) and financial investments (UK) are used as pieces in the game (Maliukevicius, 2006).

The third level concerns engagement in the international environment outside immediate zones of own territorial boundaries, such as participation in stabilizing and terrorism prevention efforts in Afghanistan or Africa (Council of Foreign Relations, 2013; Wallström, 2014). Choice of coalition partners and in which auspice this occurs matters geopolitically, as well as actions against international terrorism at large, including intelligence issues. Positioning oneself concerning interstate conflict in the international forum, e.g. the UN, also gives signal values in security policy.

The main difference between formulating security policy compared to other policy areas is the exclusiveness and secrecy that characterizes the business. However, foreign confidentiality is necessary to be able to pursue confidential talks with other countries and prepare joint actions. Even more important is the maintenance of confidentiality in defence issues, which is a necessity to impede an enemy's intelligence gathering and possible preparations for an attack. The need for secrecy in preliminary investigations conducted by the intelligence services and police is equally obvious to not reveal to terrorists and other adversaries what is known causing our information sources to go abate.

The necessary secrecy entails a number of serious problems such as lack of transparency and insight. Only a selected few in the state apparatus handles these issues why thorough oversight and a second opinion normally is lacking which also reduces democratic accountability. An important feature of this study is therefore to study how such decisions are handled in the state apparatus and if there are examples of how elements of pluralism and transparency that have been or might be included.

2.4. The Process

The relatively stable world order during the Cold War resulted in low willingness to change among state institutions planning for disruptive events. Basically, a *modus vivendi* with no major territorial conflicts characterized the relationship between the various intelligence services, the cabinet departments relevant for the security policy, and the military.

This is well described in incremental organization theory, based on studies of state budget processes Wildavsky (1964) found that existing budgetary bases

and structures were rarely or never questioned, as the changes that occurred were on the margin. However, this theoretical concept began to be questioned with the introduction of program budgeting and budget cuts in the United States in the 1970s and 1980s, which in turn made Wildavsky modify his theory to some degree (Lane, 1989).

Regarding the security and defence policy systems with privacy aspects and associated knowledge monopolies, it would be fairly uncontroversial to claim that the threshold for structural change in this sphere is even higher than in other policy areas.

New multifaceted threats in the Western world – non-state actors such as terrorists and organized crime - which are involved in illegal activities as human trafficking, drug smuggling, and cyber threats, began to replace the old state-based threat from the Soviet Union. It took several years before any changes began to appear regarding the relevant government intelligence and planning institutions. Only with strong external influences – such as 9/11 and the information revolution where telephony and IP traffic went from satellites to fibre optics – some major internal and external structural changes took place within the intelligence communities.

The elimination of one problem can actually spark other problems to evolve. We may not see them coming as there is a sense of jubilation and victory. For example president George W. Bush's triumphant declaration under the banner "Mission accomplished" on board an aircraft carrier after the successful conclusion to the high intensity regular war against the forces of Iraq's Saddam Hussein in 2003 (CNN, 2003). This was short lived after the low-intensity irregular war emerged a short time later. The same references could be observed to events during "The Arab Spring" in Libya, Egypt etc.

In the United States after 9/11, state structures on the planning side were affected mainly by the creation of the large-scale Department of Homeland Security (DHS), whereas previous systematic attempts to change the "input" and "output" structures - in the light of estimated counterterrorism and IT threats in the 1990s (Marsh Commission and PDD 62+63) – hardly had any direct impact.

The need for readjustment became particularly significant as "The Global War on Terrorism" (GWOT) began after the 9/11 attacks in late 2001. New coordinating bodies at the political and agency level, both nationally and internationally, were added, while the basic structure of government agencies were largely untouched. However, within the intelligence community, the existing cultures and working procedures needed to be challenged and reformed.

On the analysis side, conditions had changed with the new terrorism focus in relation to the Cold War, the target was no longer a single state and its internal processes, but now obscure non-state actors without limits. Opportunities for non-conventional aggressions and suicide attacks by religiously inspired groups and individuals – as opposed to strictly organized terrorist groups with

a territorial focus as PIRA and ETA – required new knowledge disciplines (religion history, cultural anthropology, etc.) and analytical methods (Ranstorp & Brun, 2013; Council of Foreign Relations, 2012; Svenska Dagbladet, 2011).

The main conclusion from the 9/11 Commission report (2002:339) was that the U.S. intelligence system (including the FBI) “lacked the imagination” to anticipate the attacks. Another criticism was the inability to collaborate and pool the available information that existed at various places in the intelligence system but could not be communicated between “stovepipes”. Even within government institutions, such as the FBI, there was information available at various levels but that never got compiled into a holistic threat picture or context.

A lesson learned is the establishment of so-called “fusion centres” in several Western countries, where different types of intelligence and security services, and sometimes even customs, coast guard, etc., are co-located to collectively process information relating to terrorist threats in order to streamline the threat and response measures (Persson, 2013). Keeping in mind that this was the result of an external event, while change and adaptation projects initiated from within is harder to find (some examples can be found in the article “Understanding Intelligence Community Innovation in the Post 9/11 World” in section B).

On the collection side, the readjustment due to GWOT was the most radical as the problem no longer was the difficulty to access secret information (“pieces of the puzzle”). Now there was open information in abundance, but it was all about weeding out the “noise” in the gigantic amounts of information to find not just a needle in the haystack but the right straw (Gorman 2008). Thus, the challenges for the design of an ideal scheduling system to anticipate possible new and old (antagonistic) threats is about – given especially exogenous external changes – optimizing both “input” structures in the form of competent intelligence organizations and “output” structures with implementing agencies.

In the former case, the political-administrative level requires proper purchasing skills towards the intelligence community. In the latter case, the political-administrative level needs a clear planning function that quickly gives lucid directions to the societal authorities that are supposed to implement protective measures against these threats. The link between “threat” and “planning” becomes an iterative bureaucratic process with a number of challenges and bottlenecks. The existence of a clear process and structure in the “policy environment” is central here.

2.5. Delimitations

A first delimitation of the study is towards non-antagonistic threats such as natural disasters etc., as well as towards reactive stochastic “disasters” such as 9/11. The event itself led to external influence through the 9/11 Commission report (2002) which tried to correct the system from the outside. Instead this dissertation focuses on the self-initiated inclination to change occurring after the Cold War. A second delimitation is towards prospective studies (“foresight”),

which focuses upon long-term time horizons (15-20 years), whilst the intelligence phenomena addressed here focuses on the intelligence community's main threat perspective in the short (2-5 years) and medium-term (5-10 years). Likewise, there is a third delimitation towards the more traditional military geopolitical threats that traditionally constitute the core for intelligence services, and instead focus is on "new threats" (IT, terrorism) that requires greater institutional adaptability.

2.6. Research and literature review

As the process from identification of threats to the implementation of protective measures is quite inaccessible and being situated in the state power's innermost core, the research and theory situation is for these obvious reasons rather thin.

Still there are some examples where individual sub-processes have been described in academic terms, however, in a US context. The three sections below firstly address the discovery and identification of threats ("Early Warning") as discussed in the intelligence literature – often linked to the field of International Relations, as well as "Management". An important work here is Roberta Wohlstetter's *Pearl Harbor: Warning and Decision* (1962) on the failures of "connecting the dots" already in the 1940's:

If our intelligence systems and all our other channels of information failed to produce an accurate image of Japanese intentions and capabilities, it was not for want of the relevant materials. Never before have we had so complete an intelligence picture of the enemy (1962:400).

Thereafter, the literature examines (not time-critically) decision-making in the policy process in which the academic studies might be captured within the political science literature on "Public Policy". Finally, the research also touches upon public administration ("Public Policy/Public Administration") and how these decisions are processed and implemented.

Some general questions can be discerned in Trevorton and Agrell (2009) and Wildavsky (1964), but still no one has managed to describe the bigger picture in this kind of public administration inertia, which often is based on an even more rigid budget process (Caiden & White, 1995).

A less successful attempt to theoretically try to argue the position of bureaucratic "threat mongers" has also been identified (Eriksson, 2001). The thesis here about "securitization" of the IT-threat in Sweden based in the state apparatus was though tainted, as the driving forces in reality came from the periphery (Parliament and non-establishment actors) and not the security policy establishment. A more fruitful approach – which also may serve as delimitation for my focus – is provided by Thomas Birkland (2006) who looked at how policy and "the process of learning" changes after major disastrous events. Specifically, 9/11 is mentioned here and the subsequent 9/11 Commission Report (2002)

with its extensive recommendations and directions, but the emphasis is on other non-antagonistic events such as Chernobyl, Hurricane Katrina, etc.

2.6.1. Threat/detection (Intelligence)

In regards to the first “input” part of the decision chain under study, there are some studies that describe the dynamics of the intelligence system and its need for flexibility to be able to adapt to a new kind of threat environment. However, concerning intelligence studies there is an emphasis on single case studies rather than comparative studies in-between countries, and for the most part the studies focuses on, in this context, the relatively transparent United States, while cases studies on other countries are not as well developed (Hastedt, 1991).

The concept “Revolution in Intelligence Affairs” (RIA) was transferred into the debate around 2005, piggybacking on the former term for the change in military organizations after the Cold War – “Revolution in Military Affairs” (RMA). Among other things, the debate emphasizes the need for experimentation and risk, as well as creating the “architects of change”⁶ (Barger, 2005). Meanwhile, voices from the outside the Intelligence Communities (IC) were raised arguing that it is not enough to share information from the IC to other non-traditional customers without integrated collaboration and co-alignment with instances of law enforcement, customs, etc. (Harrison, 2006).

The bulk of the academic literature in this area concerns intelligence analysis and its methodology. It is often argued that positivism and behaviourism fit badly with intelligence analysis, as there are too many unknown factors for a methodologically secure manner to measure and theorize about it. This is especially true for the postmodernist approach, which, therefore, assumes that it is not possible to create a theory of intelligence, but only strive for better understanding (Gill & Pythian, 2004). Another approach is the statistically oriented Bayesian method, which is more suited for graphic presentations than analysis (Laquer, 1985).

Of course there are also some threats and events (“Black Swans”⁷) that hardly can be expected to detected such as the 22 July-attack in Norway 2011. It was here the self-radicalized right-wing activist Anders Behring Breivik who first bombed the government quarters in Oslo and later killed 77 people - of which 34 were between 14-17 years - in a youth camp at Utöya (BBC 2012). Professor Wilhelm Agrell has analysed the mechanisms within the security apparatus that permit such an individual to go undetected “under the radar”, even if the same situation should repeat itself (Agrell, 2013).

⁶ Roughly, central individuals in an organization that have clear ideas and advocate change/renewal of structures and working methods.

⁷ The term describing highly improbable events was launched by Nassim Nicholas Taleb (Taleb, 2007).

2.6.2. *The policy process (“the Missing Link”)*

The policy process is key in identifying unnecessary bureaucratic gaps or seams, and as described in the beginning of this chapter, it can be divided into three sub-sections – the requirement and evaluation of information and assessments provided by the intelligence community, the generation and selection of decision alternatives, as well as finally planning directives to the administration/bureaucracy to implement.

In the United States, there are additional elements, such as public policy think tanks for “input” to the policy process (McGann, 2007). Their role in this area seems to be overlooked and under researched, which is why this special type of actor deserves to be studied closer within the framework of this dissertation. Think tanks are especially useful because they complement both the intelligence community’s assessments, as well as the remaining two sub-sections of generating decision alternatives for planning/implementation guidance.

The established role of think tanks in the US political system in an ancillary way is an attempt to compensate for the non-parliamentarian model (e.g., of Western Europe and Canada), especially as a research and analytical support mechanism for members of the US Congress who not are supported by robust political party machineries. Examples include The Heritage Foundation for the Republican Party and the Center for American Progress for certain elements of the Democratic Party.

Nevertheless, the US Congress does though have a robust research institution of its own – and which is also congressionally funded – that in many ways is comparable to a think tank: the Congressional Research Service (CRS). CRS is mandated by Congress to approach its research topics from a variety of perspectives and examine all sides of an issue, as opposed to offering partisan policy recommendations. CRS’s staff thus analyzes current policies that affect Congressional legislation and other interests and presents the impact of policy alternatives, without taking a stand on them. CRS research and analytical services come in many forms, such as reports on major policy issues, tailored confidential memoranda to members of Congress, briefings and consultations, seminars and workshops, expert congressional testimony and responses to individual inquiries.

The main difference between the private think tanks and CRS is that CRS, as a bipartisan entity, must not present policy advice or suggests policy directions. While this should not be seen as a public policy limitation, since CRS still provides an important support to Congress, it does create a “market” opportunity for the private think tanks, as different policies with the latter could be “benchmarked” and debated more thoroughly (CRS, 2015). At the same time, however, due to their non-profit and charitable tax code, even think tanks are prohibited from engaging in partisan political activities, such as supporting political candidates.

The think tanks also serve as a “revolving door” where political appointees of an outgoing administration could reside until the next election, when they are able to obtain funding for such positions (Think Tank Watch, 2012). The most precious value of a successful Think Tank is their reputation of integrity and expertise, although in recent years this has come to be questioned (see Article 5.2).

Thus, the process can be described theoretically, but the actual organization is often fluid and ad hoc, and in the United States characterized by the four-year presidential periods. There is also a risk of “politicization” of intelligence assessments in the relationship between the intelligence process and the policy process. This can happen either directly through subjective interpretations from the policy side, or indirectly as the management level in the intelligence community “adapt” the results to the expected political environment and reception (Warner, 2007).

The links between the intelligence process and the policy process, and their different focuses, are described well in the table below (Treverton & Ghez, 2012). An important difference in the examination of the inertia in the decision chain and the link between intelligence and the policy process above is that the intelligence community focuses on foreign countries while decision makers are interested in the impact upon domestic politics.

The second sub-section within the policy process – the generation and selection of decision alternatives – is the most unpredictable element, as it partly concerns political preferences, connections of individuals, constituencies, national organizations/companies and other cabinet departments or commitments to other countries. Not least when it comes to decisions with financial and organizational consequences it often becomes a budget negotiation within the government apparatus.

As previously noted, the incremental vision constitutes an important explanatory basis as both Wildavsky (1964) and Berry (1990), among others, previously have described. In other words, existing budget areas are not questioned as new additions occur on the margin, and a significant redistribution between different ministries/departments is extremely rare. In the United States the Congress has both a strong and detailed steering role in the budget process, which must also be taken into account here. Thus, incrementalism underscores that the policy process – and thereby the increasing willingness to change – might be just as disadvantageous as the inertia of public administration.

It is also in the second sub-section that think tanks in the United States appear to have the most impact by analysing different decision alternatives, and here contribute to a unique pluralism (which articles 5.1 and 5.2 covers).

When it comes to time-critical decisions that primarily do not have financial consequences, there are other examples of breath in decision-making such as “multiple advocacy” (George & Stern, 2002). This mainly concerns “second opinion” functions outside the ordinary chain of command-structures in the

Contrasting Intelligence and Policy Cultures

Intelligence	Policy
Focuses on “over there,” foreign countries.	Focuses on “here,” policy process in Washington.
Reflective, wants to understand.	Active, wants to make a difference.
Strives to suppress own views, biases, and ideology.	Acts on strong views, biases, and ideologies, at least some of the time.
Time horizon is relatively long.	Time horizon is short; an assistant secretary’s average tenure is about two years. ^a
Improves analytic products with time.	Wants assistance “yesterday.”
Understands the complexity of the world, perhaps overstating it.	Wants (and is wont) to simplify.
Knows that sharp answers or predictions will be wrong; spells out scenarios and probabilities instead.	Ideally, wants “the” answer.
Tends to take the world as given: it is there to be understood.	Tends to take the world as malleable: it is there to be shaped.
Tends to be sceptical of how much U.S. action can affect the world.	Tends to overstate what the United States (and policy itself) can accomplish.
Works in an almost entirely written culture.	Works in a culture that is significantly oral.

^a This is an estimate across the entire government. In the George H. W. Bush and Clinton administrations, the median tenure of cabinet officers was 2.5 years and that of the immediate subcabinet level was 2.3 years; one-quarter of the officers served less than 18 months. For a nice summary, see M. Dull and P. S. Roberts, “Continuity, Competence, and the Succession of Senate-Confirmed Agency Appointees, 1989–2009,” *Presidential Studies Quarterly*, Vol. 39, 2009, pp. 432–453. Although these numbers have not changed much over time, there are large variations across agencies and positions.

Figure 1: Contrasting Intelligence and Policy Cultures

United States President’s immediate surroundings – such as John F Kennedy’s chosen advisor at the Bay of Pigs invasion, “EXCON” during the Cuban Missiles Crisis, as well as Lyndon Johnson having the habit of using a “devil’s advocate” in major decisions with a foreign policy character.

It deserves to be mentioned here that although the examples above are from the US, both the time critical and the non-time critical examples also might have a generic interest for government machinery’s in other Western democracies.

In the third sub-section – planning directives to the administration/bureaucracy – one can identify where the real executive power resides. In some countries, this function has been relocated from the highest policy level (Cabinet Offices) to the level of the government agencies, given that politicians want to present to the voters a small and downsized Cabinet Office simultaneously as they require cutbacks in other government commitments and welfare systems.

In the United States the White House administration, in close proximity to the President, has a limited role relative to the departments. The President still though has through his/her power of appointment the possibility of direct control of both Secretaries of the Departments, as well as even three to four levels of politically appointed officials beneath this level, if something was to be considered to go in a completely the wrong direction. It is found in the relations of the agency level below where tension arises.

If the policy making level disposes relevant planning divisions for their business there is clearly a better chance for controlling the underlying bureaucracies, that almost always have a vested interest in maintaining the status quo (Forester, 1982:68; Halperin, Clapp & Kanter, 2006:99).

The relations between these three sub-sections on the level of the Cabinet Office appear to be highly variable between different countries, and in some cases these relations are not very transparent. An assumption here is that a systematic context often is missing when it comes to combine threat and planning perspectives in bureaucratic handling – notably, the third sub-section at the policy level regarding planning – hence, “The Missing Link”.

2.6.3. Implementation/bureaucracy

Article 1 (*Shielding the Net – understanding the issue of vulnerability and threat to the information society*) in the dissertation’s part B illustrates the problem discussed above – that the politicians own the policy while the bureaucracy usually own implementation. Another important observation is that the national security in different areas of society – for example the vulnerabilities in IT systems – is associated with large technical uncertainties and complexities and therefore seems not to be viewed in a wider threat context as when the risk is perceived as strong and challenging (Goldman, 2001:65).

One IT-incident within a single company (malware, virus or design/installation faults) can have large unexpected cascading effects far outside the company itself and affect critical societal functions like power grids, stock exchanges and communications like the big outage in North America 2003 (US and Canada Power Outage Task Force, 2004). It is very rare with governmental critical information infrastructure dependability analysis and the gap between government and the private sector concerning these kinds of responsibilities seems widened with the New Public Management influences and outsourcing.

The economic values seem to have superseded other values like public safety and security, with more of bureaucratically “stove pipes” and less of a holistic horizontal and resilient approach (Hood, 1991:11). Beside unintended threats due to complexities there are thus always opportunities for antagonistic insiders who can exploit these weaknesses, which are out of the scope and resources for intelligence and security services to look for.

The fundamental scholarly work on bureaucracy’s role within governments was written by Max Weber, in which he saw bureaucracy’s role confined to implementing laws and regulations, and not to create new rules and activities.

Also, Weber claimed that the bureaucracy is hard to control and that the politician emerges as a “dilettante” in relation to the bureaucratic expert (Gerth & Mills, 1946).

The questions thus arise why there seems to be inertia in bureaucracy and why they cannot deliver decisions in accordance to the direction disseminated by the policy level? A number of adumbrative traits that explains these shortcomings have been described by James Wilson (1989):

- Inefficiency in the public sector depends on bureaucratic rules and procedures such as norms, rules, reward systems, goals, constraints, culture and values.
- Government agencies are not independent companies meaning that incentives and reward systems are different from those in private enterprise.
- Government agencies may not retain profits or receive benefits through the organizations possibilities to earn or increased efficiency.
- Organizational design is not determined by its own agency administration.
- The organization’s goals and objectives are not determined by the organization itself.
- There is a tendency to focus and worry about processes rather than outcomes.
- Legality and uniformity is more important than efficiency for several government activities.
- The various limitations and restrictions pertaining to the public sector make it much more risk averse.
- Public organizations tend to have more managers than equivalent private sector organizations with similar functions.

When it comes to the bureaucrats’ willingness to change its own organization and activities some problems might occur because “The bureaucratic system is basically inert; it moves only when pushed hard and persistently. The majority of bureaucrats prefer to maintain the status quo, and at any one time only a small group is advocating change.” (Halperin, Clapp & Kanter, 2006:99).

A decision-making process may be ignited and affected by dramatic events and circumstances initiated by states or other external actors, new technology, changed public perceptions of societal development or bureaucracy, routine reassessments, change of managers/staff, or self-initiated actions (Halperin, Clapp & Kanter, 2006:101-105).

For change to succeed, John Thompson (1995) claims that all concerned parties should recognize the need for change. The ideal state requires permission to experiment, as well as being allowed to learn from failures and thus be able to adapt quickly to changing circumstances and new opportunities.

Wilson (1989) on the other hand, put forward some successful and perhaps somewhat paradoxical examples and traits on how organizations within the

state's core activities have updated and changed themselves without much outside pressure:

The most dramatic and revealing stories of bureaucratic innovation are therefore found in organisations – the Navy, the Marine Corps, the FBI – that have acquired settled habits and comfortable routines. Innovation in these cases requires an exercise of judgement, personal skill, and misdirection, qualities that are rare among government executives. And so innovation is rare (1989:232).

A factor in this context may be that competition, between armed services to acquire new weapons and capacities for example, contribute to a greater willingness to change. When aspects of cyber defence became a current element in the American debate, rivalry almost erupted between the armed services to become the first and principal actor in this area. In fact, Cyber Defence programs were the only programs who obtained new budgets for development and more resources when others awaited cuts for existing weapons programs (Navy Cyber Power, 2012).

If the discussion becomes even more qualified by discussing non time-critical threats (e.g. structural threats to the information society), which are cross-sectional and involve several agencies, complexity increases as bureaucracy is not a monolith, which Allison and Halperin (1972) points out:

- “Bureaucracy: the ‘maker’ of government policy is not one calculating decision-maker, but rather a conglomerate of large organisations and political actors who differ substantially about what their government should do on any particular issue and who compete in attempting to affect both government decisions and the actions of their government.” (1972:42).
- “Both the bargaining and the results are importantly affected by a number of constraints, in particular, organisational processes and shared values.” (1972:43).

All in all, therefore, policy making pluralism seems to be able to arise among established bureaucracies when sensing competition within the government apparatus for funding resources and other types of influence, which possibly could be utilized by the superior policy environment in order to generate a greater variety of decision-making and orientation options.

2.6.4. Summary research design

The overall picture of the research situation on the relations between the threat and planning processes is that there is a broad and established tradition of research concerning the administrative area and the inner workings of the bureaucracy, often emanating in Weber's ground-breaking work *Economy and Society* from 1922.

Research in the policy area has often focused on two areas, either the transfer of political will (policy) into financial terms or the relatively young research area in crisis management – i.e. time-critical situations of decision-making –

where perhaps Graham Allison's *Essence of Decision* from 1971 paved the way for today's extensive research arena.

Among the three sub-areas under study the intelligence research is the youngest, in which there are two traditions. Firstly, a less historically focused line of research about "post mortems" reviews of policy decisions on the basis of released intelligence documents. Secondly, a larger tradition based in political science that for example evaluates the usefulness of various methods of analysis to predict relevant global developments and threats. There is also a close link to the ability of the policy process to absorb impartial intelligence assessments in relation to "politicizing" them. Sometimes practitioners question the word intelligence research, as the collection part within this field is considered more of an art than a science.

As already noted, these are, however, three areas that normally are not coupled in a thematic way in terms of research. These should now be presented and discussed.

3. Policy adaption within the national security environment

The policy processes within the national security environments can be studied from two directions – what do the existing postures look like, and how adaptable is it to potential upcoming challenges.

3.1. The model of analysis for security policy ("the decision chain")

Within security policy the abovementioned process is scaled down concerning actors and flows. One theme in this dissertation is to study factors that cause delay in the decision chain "Detection-Action-Recommendation-Decision-Implementation" in relation to new societal antagonistic threats such as IT threats or terrorism. This decision chain is also used in Article 1 as the analytic frame. The following description is based in a generic Swedish/Western European context, but as we shall see where the United States constitutes a special case.

In the article 1 (*Shielding the Net – understanding the issue of vulnerability and threat to the information society*) it was established that some countries had a shorter reaction timeline (N) from detection of a potential threat to implementation of protective measures than others. What did these countries have in common and what constituted this factor X that gave them this faster pace?

The main components in this decision chain consist of the following elements:

Part A Threat detection ("input") can largely be attributed to the intelligence community's (including the security services) responsibility of how to detect/perceive new trends and tendencies. Inertias – bureaucratic rigidities, "group think" and too specific directions – can within this system mean that important signals are missed, and that for instance the assigned researchers

can come up with important new angles to a problem or other contributions. Alternatively, no one notices the “Black Swan”-events.

Part B The policy process (“the Missing Link”) can be divided into three separate parts:

- 1. Policy planning (actions and recommendations) based on intelligence material (“raw” and processed).
- 2. Policy decisions where the recommendations will be put in context and de-conflicted with other previous or planned policies including budgetary issues.
- 3. Planning directives for the administration/agencies to guide the implementation of the decided policy.

The Cabinet Offices/National Security Councils will normally process a new or unanticipated threat – observed by the intelligence community or other sources of knowledge – with the assigning of a commission or an investigation

Article 1.

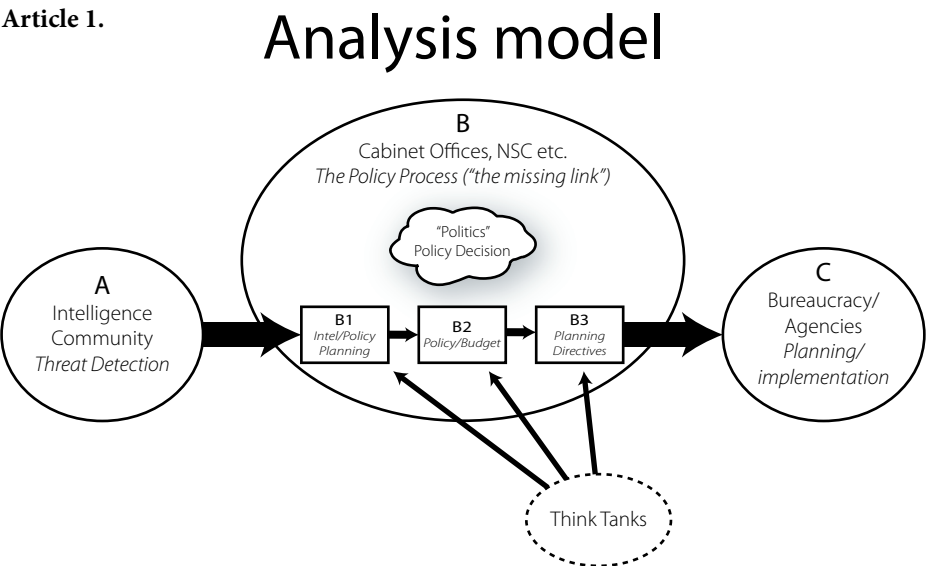
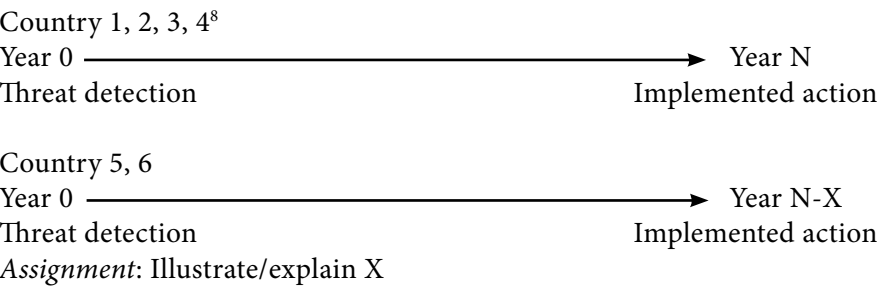


Figure 2: Analysis model Intelligence-Policy-Implementation



8

These countries are described more concretely in article 1.

constituted of politicians or senior officials. When the investigation is complete it usually results in some findings and recommendations. These findings are often sent to concerned agencies and in some cases to NGO's, for additional views and input, thereafter, a bill is processed within the Cabinet Department before being sent for approval to the Parliament/Congress. Unfortunately, it is in the national security field more common with sweeping "post mortem"-inquiries like the 9/11 Commission or the Benghazi-report in US, while the inductive pro-active investigations on for example evolving strategic challenges (China policy, cyber threats etc.) are more low-key.

In this rather non-transparent process there will be a first match between "threat" versus "planning" as the specific threat and its consequences will both in Europe and in US be assigned to one specific lead Cabinet Department (Department of Defence, Department of Justice etc.). In particular, financial and budget effects are for the first time tentatively assessed, as well as the Department of Finance adding their restrictions to the directives for the investigation. Normally, the new directives must be cost-neutral within the national budget and managed within the existing budget limits of the specifically assigned Cabinet Department.

When in Parliament or in Congress, Cabinet Ministers/Secretaries often want to show decisiveness and quickly present actionable proposals for the elected officials, however, their own Cabinet Department machinery may have another or even a conflicting agenda. In the dialogue with their agencies there is a tendency for desk officers within the Cabinet Departments to be less precise in detailed actions, and instead have more leeway to deal with this in the yearly budget dialogue.

The agencies, on the other hand, seldom want an added mission or assignment that conflicts or reallocates resources from the existing ones – especially, if it demands a changed competence structure within the agency staff, as that is a long-term process. As the bureaucracy, Weber pointed out, normally have the upper hand against the policy machinery. The Cabinet officials know that it often will be a tough bargain and that they need time to integrate these types of planning directives in the annual budget directives for the agencies.

The bureaucracy's upper hand, in comparison to the policy machinery, can be explained by more staff for the production of memos with facts, assessments and consequence analysis, a deeper subject matter expertise, and – when it comes to security and defence related matters – a "knowledge monopoly". This implies a reactive mode for the policy machinery where they can only react – and in some cases maybe execute marginal changes – on a single proposal, suggestion or an initiative on certain issues from the bureaucracy, instead of having several views and opinions. The American system with its think tanks is, as we will see later, an interesting exception among the Western countries.

Part C Implementation ("output") concerns how bureaucracy finally implements policy decisions through converting allocated funds and directions into

new security measures, rules, regulations and supervisory practices. Here, agency executives might have to refocus the business, hire new employees and/or lay off staff and consultants, while they might have to enter other agencies' areas of responsibility for the proposed security measure to obtain full effect.

If this analysis model is to be further decomposed, the policy process (**B**) can be divided into three sub-parts. **B1** manages the contacts with the intelligence community both in terms of receiving intelligence as well as to provide intelligence requirements ("order"). **B2** is the part where the current policy stance is coordinated and balanced against other budget areas. For example, if there are perennial budgets in these, there will be more civil servant influence here in relation to these decisions being calibrated afresh annually in the general budget preparation. **B3** is the planning function which in dialogue with the agency level should translate the directions from the policy process so that they are implemented as intended, and not leaving room for alternative interpretations that the bureaucracy, in their own organizational interest, may prefer.

With this background, it is important to look at how the empirical data concerning challenges in the form of new threats and their characteristics developed.

3.2. Challenges for the security policy process concerning new threats

The two most significant new types of threats are terrorism and cyber threats – both of which have the attribute of being cross-sectorial and involve areas of responsibility within several ministries and agencies. In some countries various aspects of terrorism are handled by four different ministers as well as by up to ten agencies,⁹ without coordination among the involved parties. Regarding protection against cyber threats, it is in Sweden at least four ministries and eight agencies¹⁰ sharing different aspects of responsibility without an efficient overall coordination. Other relevant countries like the United Kingdom, Finland, Norway and the Netherlands have far less fragmented approaches (Nicander, 2010).

The new threats are also "civil" in nature – i.e. they are not only part of the military organization and the mission of the Armed Forces. Terrorism mainly affects the police and crisis management agencies, as well as local authorities

9 *Cabinet Offices:* the Prime minister's Office, the Department of Justice, the Departments of Defence, and the Ministry for Foreign Affairs.

Government Agencies: the Security Service, the Armed Forces/the Military Intelligence and Security Directorate, the National Defence Radio Establishment, the National Police Board/the National Bureau of Investigation, the Civil Contingencies Agency, the Coast Guard, The Prison and Probation Service, the Radiation Safety Authority, the Migration Board, the Prosecution Authority.

10 *Cabinet Offices:* the Department of Defence, the Department of Justice, the Ministry for Foreign Affairs, the Department of Enterprise, Energy and Communications.

Government Agencies: the Security Service, the Armed Forces, the National Defence Radio Establishment, the National Police Board/the National Bureau of Investigation, the Civil Contingencies Agency, the Data Inspection Board, the National Board of Health and Welfare, the Financial Supervisory Authority.

regarding preventive measures, however military organizations can provide some support such as foreign intelligence, bomb disposal etc. Information Assurance and Cyber Security deals with the society's information critical information infrastructure, but where there exists neither a direct link to publicly planned preparedness measures.

These two types of new threats have a rapid course of action as opposed to a gradually growing geostrategic tension in an adjacent area, which gives the concerned military forces time in a prepared fashion to raise the costly emergency measures. A terrorist attack, similar to the one in Stockholm in December 2010 where the Swedish terrorist was radicalized in England (Dagens Nyheter, 2013) - or even the siege of the West-German Embassy in Stockholm 1975 (Hansén & Nordqvist, 2006) – may have had only a very vague warning in advance and the attacks were boundless by nature. Such threats, therefore, cannot be completely prevented as they often are what are termed transferred threats (i.e., originating in one country but taking place in another).

The Mohammed Cartoon-incident, which resulted in attacks on Swedish diplomatic representations abroad, provides an additional example of transferred threats (Dagens Nyheter, 2010). This means that an attack against Sweden does not have to depend on Swedish foreign policy actions, but can happen because, in relation to other countries, Sweden's merit is as the relatively weakest link in security – for example Israeli or American diplomats while travelling to or from the airport to their residence.

A large-scale cyber-attack on critical societal functions is also difficult to predict. Aside from the fact that it will most likely be anonymous, it will also be rapid and take place within seconds before any organized crisis management is likely to have the opportunity to come around.

In both these cases, coordination of society's response opportunities is necessary; a necessity for which public administrations in most countries is not suited. The needed coordination must come about in command structures instead of slow collaboration processes. Also, after a cyber-attack on information structures recovery measures may require faster and greater redistribution between areas of expenditure than the perennial budget processes to be able to handle detected critical vulnerabilities.

An additional factor is the lack of transparency and openness following the need for confidentiality, partly to deal with threat information in the form of intelligence, but also to not reveal possible critical vulnerabilities under protection.

The above mentioned difficulties require an organization with expertise and professionalism that are difficult to access on the open labour market, and which cannot be solved with consultants and staffing companies. The need for security classified personnel also limits the selection of possible individuals suited for these positions. The demands for limited dissemination and security

perimeters on premises further limits knowledge being transfer sideways or from society in general.

4. What processes are studied and how?

This dissertation focuses on where the institutional iterative process takes place, where the “input” (mainly intelligence and defence research bodies) signals of threats and potential vulnerabilities are weighed against the “output” in the form of steering directives signals and financial support to the community structures that need to be protected and strengthened.

The articles are presented in a step-by-step process. Firstly, in article 1 (*Shielding the net – understanding the issue of vulnerability and threat to the information society*), the timelines and processes between “input” and “output” signals are analysed as a comparison between countries of the chain Detection-Action-Recommendations-Decision-Implementation, using IT/cyber threats as a “case” (please find the figure “Analysis model” in 3.1).

Secondly, in article 2 (*Understanding Intelligence Community Innovation in the Post-9/11 World*), the “input” side and pluralism in the intelligence community is studied more closely. The focus here is how key players can improve their behaviour such as providing flexibility, avoid groupthink and thought lockups when, due to reasons of confidentiality, a knowledge monopoly exist.

An example of an illustrative question formulation of when non-state actors may consider IT-based attack methods can be found in article 3 (*Information Terrorism – When and by Whom*), where the pros and cons in a terrorist modus operandi are analysed.

Articles 2 and 3.

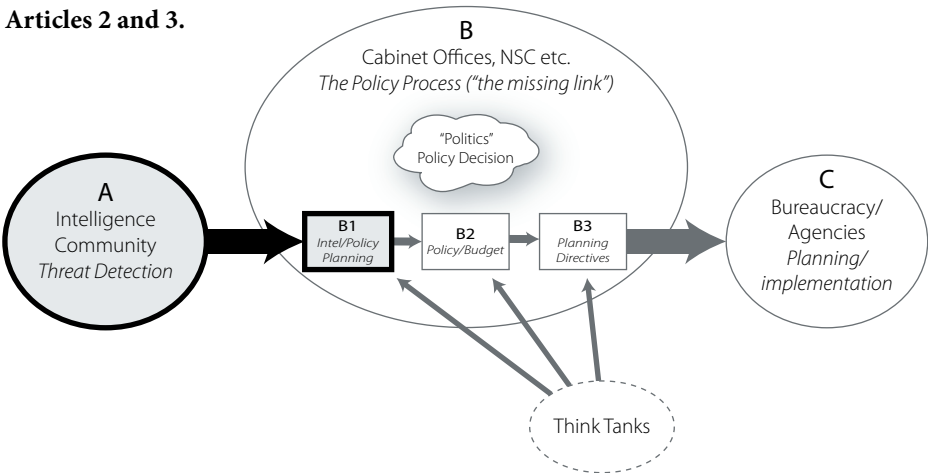


Figure 3: Relations Intelligence-Policy

The third step involves the “output” side, which begins with a short illustrative background description in article 4 (*The Trojan Horse in the Information Age*) about how the Swedish system acknowledged the IT threat, and how a

number of management challenges were identified when actions against these threats were proposed.

Article 4.

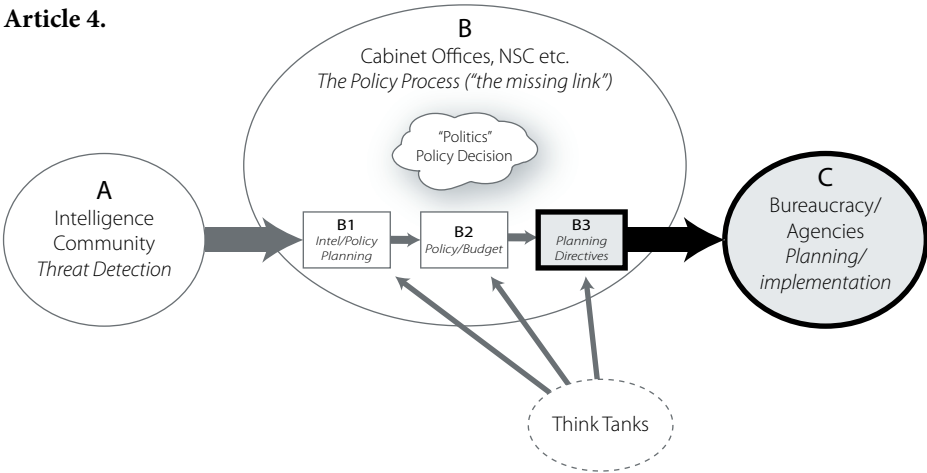


Figure 4: Relations Policy-Bureaucracy

Thereafter, an extensive review of how pluralism on the “output” side can be amplified and override existing knowledge monopolies will be provided. This is done by focusing on the specific American phenomenon of public policy think tanks and their role in advising the security policy processes.

Articles 5.1 and 5.2.

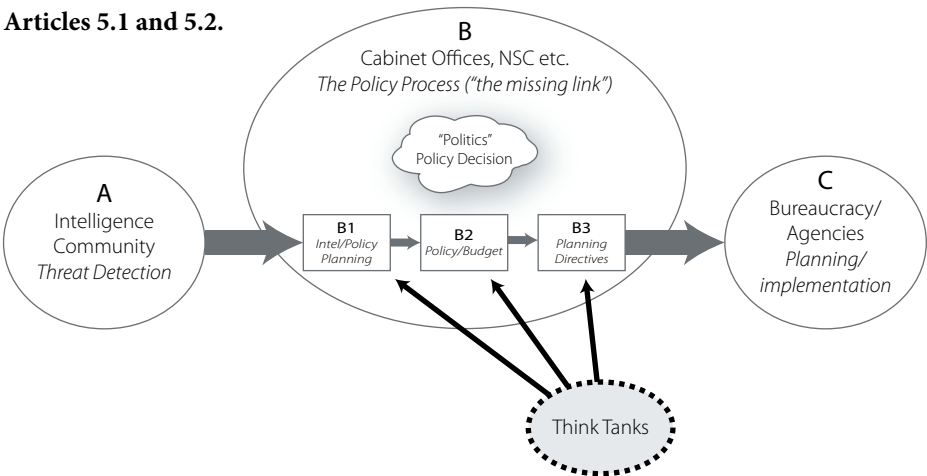


Figure 5: The impact of think tanks in the policy process

The study of think tanks is done in two steps. Firstly, article 5.1 (*The role of Think Tanks in the US Security Policy Environment – A Forgotten Actor?*) provides a theoretical analysis based on an interview survey, among personnel working in concerned agencies and ministries, about the importance of think

tanks and their role in congressional decision-making. Secondly, article 5.2. (*The Recipe for Think Tank Success: From the Insiders Perspective*) provides a more detailed analysis of think tanks' success factors based on unique insider's perspectives from active senior practitioners.

In summary, this dissertation and its articles are intended to provide a picture of all the relevant links in the security policy decision-making, from the first intelligence information via the specific closed processing procedures up to the implementation of protective measures.

Therefore, the research gaps that are filled descriptively concern innovation and adaptation to an environment in change within the closed intelligence milieu, in which external market mechanisms are lacking, as well as specific longitudinal decision-making. The phenomenon of think tanks and their role in American security policy is viewed in a new light both descriptively and exploratory. The latter through unique insights about how these think tanks are successful and affect security policy decision-making from actors "on the inside" of security policy.

Hopefully, this will also contribute to a future new theory that bridges diverse fields of science such as international relations, public administration, sociology and microeconomic theory.



This thesis now proceeds with the articles which have been briefly presented and discussed in this section. The articles' findings are thereafter summarized, discussed and related to the possible impact on enhanced policy formulating governmental processes.

References

- Agrell, Wilhelm (2013). *The Black Swan and Its Opponents: early warning aspects of the Norway attacks on 22 July 2011*. Stockholm: Swedish National Defence College/CATS.
- Allison, Graham T. (1971). *Essence of Decision: Explaining the Cuban Missile Crisis*. Boston: Little Brown.
- Allison, Graham T., & Halperin, Morton H. (1972). "Bureaucratic Politics: A Paradigm and Some Policy Implications". *World Politics* 24(S1):40-79.
- BBC (2012). "Anders Behring Breivik: Norway court finds him sane", 2012-08-24. <http://www.bbc.com/news/world-europe-19365616> Retrieved 2015-01-13.
- Barger, Deborah G. (2005). "Toward a Revolution in Intelligence Affairs". Santa Monica: RAND Corporation. http://www.rand.org/content/dam/rand/pubs/technical_reports/2005/RAND_TR242.pdf
- Beal, John Casey (2011). "Toward and Emancipatory Understanding of Global Being: An Ideological, Ontological Critique of Globality". University of Ottawa: Master Thesis. <http://www.ruor.uottawa.ca/handle/10393/20386>
- Berry, William D. (1990). "The confusing Case of Budgetary Incrementalism: Too Many Meaning for a Single Concept". *Journal of Politics* 52(1):167-196.
- Birkland, Thomas A. (2006). *Lessons of Disaster – Policy Change after Catastrophic Events*. Washington DC: Georgetown University Press.
- Boin, Arjen, Ekengren, Magnus and Rhinard, Mark (Ed.) (2013). *The European Union as Crisis Manager: Patterns and Prospects*. Cambridge: Cambridge University Press.
- Brighton, Shane (2007). "British Muslims, Multiculturalism and UK Foreign Policy: 'Integration' and 'Cohesion' in and Beyond the State". *International Affairs* 83(1):1-17.
- Brookes, Peter & Shin, Jitlye (2006). "China's influence in Africa: Implications for the United States". *Background* (1916):1-9.
- Burke, Jason (2004). "Think Again: Al Qaeda". *Foreign Policy* (142):18-26.
- Bäck, Henry et al. (2011). *Den svenska politiken – struktur, processer och resultat*. Malmö: Liber AB.
- Caiden, Naomi & White, Joseph (Ed.) (1995). *Budgeting, Policy, Politics: An Appreciation of Aaron Wildavsky*. New Jersey: Transaction Publishers.
- CIA (1995). *A consumer's guide to intelligence*. Washington DC: Diane Publishing Staff.
- Clapper, James (2015). "Intell integration key to fight against threat actors", 2015-01-09. <http://www.executivegov.com/2015/01/james-clapper-intell-integration-key-to-fight-against-threat-actors/> Retrieved 2015-01-11.
- CNN (2014). "Boko Haram Fast Facts", 2014-11-01. <http://edition.cnn.com/2014/06/09/world/boko-haram-fast-facts/> Retrieved 2014-11-05.
- "ISIS Fast Facts", 2014-10-09. <http://edition.cnn.com/2014/08/08/world/isis-fast-facts/> Retrieved 2014-11-05.
- "Presidential Decision Directives", no date given. http://www.ncrhomelandsecurity.org/security/security/otherplans/pres_dir_sum.pdf Retrieved 2014-11-04.
- CNN (2003). "Bush makes historic speech aboard warship", 2003-05-02. <http://edition.cnn.com/2003/US/05/01/bush.transcript/> Retrieved 2015-01-13.
- CRS (2013). "About us", 2013-05-01 <http://www.loc.gov/crsinfo/about/> Retrieved 2015-02-23
- Council on Foreign Relations (2013), "Issue Brief: The Global Regime for Armed Conflict", 2013-06-19. <http://www.cfr.org/peacekeeping/global-regime-armed-conflict/p24180> Retrieved 2015-01-11.
- Council of Foreign Relations (2012). "Basque Fatherland and Liberty (ETA) (Spain, separatists, Euskadi ta Askatasuna)", 2012-11-17. <http://www.cfr.org/separatist-terrorism/basque-fatherland-liberty-eta-spain-separatists-euskadi-ta-askatasuna/p9271> Retrieved 2014-11-05.
- Dagens Nyheter (2013). "Självordsbombaren fick 750 000 från CSN", 2013-02-18. <http://www.dn.se/nyheter/sverige/sjalv-mordsbombaren-fick-750000-fran-csn/> Retrieved 2015-01-11.

- Dagens Nyheter (2010). "Muhammed-karikatyrer publiceras igen", 2010-08-10. <http://www.dn.se/kultur-noje/nyheter/muhammed-karikatyrer-publiceras-igen/> Retrieved 2015-01-11.
- Daily Mail (2009). "Europe Plunged into Energy Crisis as Russia Cuts Off Gas Supplies Via Ukraine", 2009-01-07. <http://www.dailymail.co.uk/news/article-1106382/Europe-plunged-energy-crisis-Russia-cuts-gas-supply-Ukraine.html> Retrieved 2014-11-05.
- Easterby-Smith, Mark and Marjorie A. Lyles (Ed.) (2003b). "Introduction: Watersheds of Organizational Learning and Knowledge Management" in *The Blackwell Handbook of Organizational Learning and Knowledge Management*. New Jersey: Blackwell Publishing.
- Eriksson, Johan (Ed.) (2001). *Hotbildernas Politik: Hur blev IT säkerhetspolitik*. Stockholm: Utrikespolitiska institutet.
- Evans, Mark and Davies, Jonathan (1999). "Understanding Policy Transfer: A Multi-Level, Multi-Disciplinary Perspective", 77(2):361-385.
- Forester, John (1982). "Planning in the Face of Power". *Journal of the American Planning Association* 48(1):67-80.
- Fukuyama, Francis (1989). "The End of History". *The National Interest* 16(3):3-18.
- Garthoff, Douglas F. (2007). "Chapter 12: R. James Woolsey: Uncompromising Defender" in *Directors of Central Intelligence as Leaders of the U.S. Intelligence Community, 1946-2005*. Washington DC: Potomac Books, Inc.
- George, Alexander L., & Stern, Eric K. (2002). "Harnessing Conflict in Foreign Policy Making: From Devil's to Multiple Advocacy". *Presidential Studies Quarterly* 32(3):484-508.
- Gerth, Hans H., & Mills, C. Wright (1946). "Bureaucracy" in *From Max Weber: Essays in Sociology*. New York: Oxford University Press.
- Gill, Peter & Phythian, Mark (2004). "Issues in the theorisation of intelligence." *Paper presented at the International Studies Association conference in Montreal, ISA04* Proceeding 73613.
- Goldman, Emily O. (2001). "New Threats, New Identities and New Ways of War: The Sources of Change in National Security Doctrine". *Journal of Strategic Studies* 24(2):43-76.
- Gorman, Siobhan (2008). "NSA's Domestic Spying Grows As Agency Sweeps Up Data: Terror Fight Blurs Line Over Domain; Tracking Email", 2008-03-10. <http://online.wsj.com/news/articles/SB120511973377523845?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB120511973377523845.html> Retrieved 2014-11-06.
- Grigas, Agnia. (2013). *The Politics of Energy and Memory between the Baltic States and Russia*. Farnham: Ashgate.
- Gromet, Dena. M., Kunreuther, Howard, & Larrick, Richard P. (2013). "Political ideology affects energy-efficiency attitudes and choices". *Proceedings of the National Academy of Sciences* 110(23):9314-9319.
- Halperin, Morton H., Clapp, Priscilla A., & Kanter, Arnold (2006). *Bureaucratic Politics and Foreign Policy* 2nd edition. Washington DC: Brookings Institute.
- Hansén, Dan & Nordqvist, Jens (2006). *Kommando Holger Meins: Dramat på Västtyska ambassaden och Operation Leo*. Stockholm: Ordfront Förlag.
- Harrison, Fredrick, (2006). "Sharing Information is not enough". *Defense Intelligence Journal* 15(1):25-29.
- Hastedt, Glenn P. (1991). "Towards the Comparative Study of Intelligence". *Conflict Quarterly* XI(3):55-72.
- Hood, Christopher (1991). "A Public Management for All Seasons", *Public Administration* 69(1):3-19. www.ipf.se/lib/get/file.php?id=154802b4883652
- Hmielowski, Jay D. et al. (2013). "An attack on science? Media use, trust in scientists, and perceptions of global warming". *Public Understanding of Science*, 0963662513480091.
- IPCC (2014). "Climate Change 2014: Impacts, Adaptation, and Vulnerability". Geneva: Intergovernmental Panel on Climate Change. <http://ipcc-wg2.gov/AR5/>
- Koraeus, Mats (2008). "Who Knows? The Use of Knowledge Management in Crisis". *Crisis Management Europe Research Program volume 36*. Stockholm: Swedish National Defence College/CRISMART.
- Lane, Jan-Erik (1989). "Bokanmälan – Aron Wildavsky: The New Politics of the Budgetary Process". *Ekonomisk Debatt* 17(1):49-50.
- Laqueur, Walter (1985). *A World of Secrets: The Uses and Limits of Intelligence*. New York: Basic Books.

- Lindroos, Christoffer (2013). "Budgetmaximering enligt William Niskanens modell inom budgetförhandlingar mellan statliga ämbetsverk och ministerier". Helsingfors: Helsingfors universitet/Statsvetenskapliga fakulteten.
<https://www.finna.fi/Record/helka.2493223>
- Maliukevicius, Nerijus (2006). "Geopolitics and Information Warfare: Russia's Approach". *Lithuanian Strategic Annual Review*, 121-146.
- Marrin, Stephen (2002). H-Diplo, 2002-03-03.
<http://h-net.msu.edu/cgi-bin/logbrowse.pl?trx=vx&list=h-diplo&month=0203&week=a&msg=Pu1nT0UB4V8TZ%2b0ehfBsBw&user=&pw>
Retrieved 2014-04-29.
- McGann, James (2007). *Think Tanks and Policy Advice in the United States*. New York: Routledge.
- Navy Cyber Power 2020 (2012). "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense, Department of Defense".
http://www.public.navy.mil/fcc-c10f/Strategies/Navy_Cyber_Power_2020.pdf
- Nicander, Lars (2010). Shielding the Net – Understanding the Issue of Vulnerability and Threat to the Information Society." *Policy Studies* 31(3):283-300. DOI: 10.1080/01442871003615935.
- Niskanen, Jr. William A. (1994). *Bureaucracy and Public Economics*. Aldershot: Edward Elgar Publishing Limited.
- Nonaka, Ikujiro & Toyama, Ryoko (2003). "The knowledge-creating theory revisited: Knowledge creation as a synthesizing process". *Knowledge Management Research and Practice* 1(1):2-10.
- Paillard, Christophe-Alexandre (2010). "Russia and Europe's Mutual Energy Dependence". *Journal of International Affairs* 63(2): 65-84.
- PCCIP (1997). "Critical Foundations: Protecting America's Infrastructures", no date given.
<http://www.iwar.org.uk/cip/resources/pc-cip/info.html>
Retrieved 2014-11-05.
- Pham, J. Peter (2012). "Boko Haram's Evolving Threat". *Africa Security Brief* (20).
- Persson, Gudrun (2013). *Fusion Centres – Lessons Learned: a study of coordination for intelligence and security services*. Stockholm: Swedish National Defence College/CATS.
- Petersson, Olof (2006). *Svensk politik*. Stockholm: Nordstedts Juridik AB.
- Ranstorp, Magnus & Brun, Hans (2013). *Terrorism Learning and Innovation: Lessons From PIRA in Northern Ireland*. Stockholm: Swedish National Defence College.
- Rantapelkonen, Jari & Salminen, Mirva (Ed.) (2013). *The Fog of Cyber Defence*. Helsinki: National Defence University.
- Sergie, Mohammed Ali & Johnson, Toni (2014). *Boko Haram*, Council on Foreign Relations
<http://www.cfr.org/nigeria/boko-haram/p25739>
Retrieved 2014-11-05.
- Shulsky, Abram N., & Schmitt, Gary J. (2001). *Silent Warfare: Understanding the World of Intelligence* 3rd edition. New York: Brassey's.
- Simons, Greg (2010). "Fourth Generation Warfare and the Clash of Civilisations". *Journal of Islamic Studies* 21(3):391-412.
- SIS (2015). "What we do", no date given.
<https://www.sis.gov.uk/about-us/what-we-do.html>
Retrieved 2015-01-18.
- Svenska Dagbladet (2011). "Bomben Skulle ha Dödat 40 Personer", 2011-11-05.
http://www.svd.se/nyheter/inrikes/bomben-skulle-ha-dodat-40-personer_6684286.svd
Retrieved 2014-11-05.
- Speck, Ulrich (2014). "Putin planning 'Soviet Union lite'", 2014-03-04.
<http://edition.cnn.com/2014/03/03/opinion/ukraine-world-order-opinion-ulrich-speck/>
Retrieved 2014-07-10.
- Spicer, Michael W. (2001). "Value pluralism and its implications for American public administration". *Administrative Theory & Praxis* 23(4):507-528.
- Stiglitz, Joseph E. (1999). "Public policy for a knowledge economy". *Remarks at the Department for Trade and Industry and Center for Economic Policy Research* 27.
- Taleb, Nassim Nicholas (2007). "The Black Swan: The Impact of the Highly Improbable", 2007-04-22.
<http://www.nytimes.com/2007/04/22/books/chapters/0422-1st-tale.html>
Retrieved 2014-11-04.
- Think-Tank Watch (2012). "The Revolving door of Think Tanks", 2012-03-09.
<http://www.thinktankwatch.com/2012/03/state-department-study-of-think-tanks.html>
Retrieved 2015-01-13.

- Thompson, John (1995). "Participatory Approaches in Government Bureaucracies: Facilitating the Process of Institutional Change". *World Development* 23(9):1521-1554.
- Treverton, Gregory F., & Agrell, Wilhelm (Ed.) (2009). *National Intelligence Systems*. New York: Cambridge University Press.
- Treverton, Gregory F., & Ghez, Jeremy J. (2012). "Making Strategic Analysis Matter", *Conference Proceedings*. Santa Monica: RAND.
- US and Canada Power Outage Task Force (2004). "Final report on the 14 August 2003 Blackout in the United States and Canada: Causes and Recommendations", 2004-03-31.
<http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf>
Retrieved 2015-01-13.
- Wallström, Margot (2014). "Statement by the Swedish Foreign Minister", 2014-10-24.
<http://www.swedenabroad.com/en-GB/Embassies/UN-New-York/Current-affairs/Statements/United-Nations-Day---Margot-Wallstrom-delivers-a-statement-sys/>
Retrieved 2015-01-11.
- Warner, Michael (2007). "Wanted: A Definition of Intelligence", 2007-04-14.
<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol46no3/article02.html>
Retrieved 2014-04-30.
Updated 2008-06-27.
- Weber, Max (1922/1978). *Economy and society; an outline of interpretive sociology*. Berkley (CA): University of California Press.
- Wildavsky, Aaron (1964). *Politics of the Budgetary Process*. Boston: Little Brown.
- Wilson, James Q. (1989). *Bureaucracy: What Government Agencies Do and Why They Do it*. New York: Basic Books.
- Wohlstetter, Roberta (1962). *Pearl Harbor: Warning and Decision*. Stanford: Stanford University Press.
- Zausen, Leo (2014). "Heidegger's Metaphysical Affirmation: The Moods and Technologies of Dasein", 2014-04-21.
<https://oedipuswrecks.wordpress.com/2014/04/21/heideggers-metaphysical-affirmation-the-moods-and-technologies-of-dasein/>
Retrieved 2015-08-23.
- 9/11-Commission's report (2002). "The 9/11 Commission Report – final report of the national commission on terrorist attacks upon the United States". New York: W.W. Norton & Company, Inc.
<http://www.9-11commission.gov/report/911Report.pdf>